IEDF
INSTITUTO ELECTORAL DEL DISTRITO FEDERAL

Memoria del Simposio acerca de las urnas electrónicas para la emisión del voto ciudadano

Memoria del Simposio acerca de las urnas electrónicas para la emisión del voto ciudadano

Consejo General del Instituto Electoral del Distrito Federal

Consejero presidente
Javier Santiago Castillo

Consejeros electorales
Bernardo Fernández del Castillo
María Elena Homs Tirado
Eduardo Huchim May
Rubén Lara León
Rosa María Mirón Lince
Juan Francisco Reyes del Campillo Lona

Secretario ejecutivo
Adolfo Riva Palacio Neri

REPRESENTANTES DE LOS PARTIDOS POLÍTICOS

Partido Acción Nacional
Ernesto Herrera Tovar, propietario
Raúl Herrera Espinosa, suplente

Partido Revolucionario Institucional
Marco Antonio Michel Díaz, propietario
Juan Manuel Vicario Rosas, suplente

Partido de la Revolución Democrática
Juan González Romero, propietario
Felipe Pérez Acevedo, suplente

Partido del Trabajo
Ernesto Villarreal Cantú, propietario
Adrián Pedro Cortes, suplente

Partido Verde Ecologista de México
Jorge Legorreta Ordorica, propietario
Zuly Feria Valencia, suplente

Convergencia
Armando Levy Aguirre, propietario
Hugo Mauricio Calderón Arriaga, suplente

Nueva Alianza
Jesús Enrique Díaz Infante Chapa, propietario
Miguel Ángel Arnaiz Mancebo del Castillo, suplente

Alternativa Socialdemócrata y Campesina
Carla Alejandra SánchezArmas García, propietaria
Salvador González Briseño, suplente

D I R E C T O R I O

Comisión de Organización y Geografía Electoral
María Elena Homs Tirado, presidenta
Bernardo Fernández del Castillo, integrante
Rubén Lara León, integrante

Iván Huesca Licona
Director ejecutivo de Organización y Geografía Electoral

Rodolfo Torres Velázquez
Titular de la Unidad de Informática

Coordinación editorial
Unidad de Documentación
Claudia Sofía Irazoque Palazuelos, subdirectora de Difusión y Publicaciones
Unidad de Informática
Azalia Rodríguez Abundis, jefa del Departamento de Desarrollo de Sistemas 2

Corrección de estilo
Unidad de Documentación
Claudia Sofía Irazoque Palazuelos, subdirectora de Difusión y Publicaciones
Karina Rosalía Flores Hernández, analista "A"

Fotografías
Unidad de Comunicación Social
Verónica Ávila Gallegos, analista "A"
Miguel Ángel Valera Márquez, asistente operativo

Diseño de portada
Unidad de Comunicación Social
José Luis Martínez Villarreal, asistente operativo

La Comisión de Organización y Geografía Electoral del IEDF en su sexta sesión ordinaria del 10 de septiembre de 2004, instruyó a las áreas responsables de la organización del Simposio acerca de las urnas electrónicas para la emisión del voto ciudadano elaborar las memorias gráfica, audiovisual e impresa.

D.R. Instituto Electoral del Distrito Federal
Dirección Ejecutiva de Organización y Geografía Electoral y la Unidad de Informática
Huizaches número 25, colonia Rancho los Colorines, delegación Tlalpan, México, D.F.
código postal 14386
1a. edición, noviembre de 2005
ISBN: 970-786-003-0
Ejemplar de distribución gratuita, prohibida su venta
Impreso y hecho en México

ÍNDICE

PRESENTACIÓN

El Instituto Electoral del Distrito Federal (IEDF), en el marco del *Programa particular en materia de automatización de los procesos electorales*, ha realizado desde hace cuatro años diversos trabajos de investigación orientados a conocer los diferentes tipos de tecnologías aplicadas a la emisión y cómputo de votos, y las experiencias organizativas de las instituciones electorales de países que han utilizado aditamentos electrónicos en sus procesos comiciales y de participación ciudadana.

En este contexto, el IEDF a través de la Comisión de Organización y Geografía Electoral y con el apoyo de la Dirección Ejecutiva de Organización y Geografía Electoral y de la Unidad de Informática, organizó el 2 y 3 de septiembre de 2004, el *Simposio acerca de las urnas electrónicas para la emisión del voto ciudadano*, con el propósito de analizar, desde una perspectiva teórico-conceptual, el uso de urnas electrónicas en procesos electorales y de participación ciudadana.

Participaron 33 especialistas en voto electrónico de los ámbitos académico, electoral y empresarial, quienes a partir de una visión crítica enriquecieron el análisis de los temas relativos al diseño e implementación de sistemas de votación basados en el uso de las urnas electrónicas.

Los temas analizados en el Simposio se abordaron en cuatro mesas de trabajo: *1)* Seguridad en el uso de urnas electrónicas, *2)* Aspectos jurídicos, sociales, políticos, procedimentales, logísticos y de capacitación en el uso de urnas electrónicas, *3)* Confiabilidad y auditabilidad de las urnas electrónicas y, *4)* Experiencia en el diseño de urnas electrónicas.

Además, se presentaron los avances en la construcción de prototipos de urnas electrónicas, diseñados para el Instituto Electoral del Distrito Federal por la Universidad Nacional Autónoma de México, el Instituto Politécnico Nacional, la Universidad Autónoma Metropolitana, y el Instituto

Tecnológico y de Estudios Superiores de Monterrey campus Ciudad de México. También se dieron a conocer los modelos de urna electrónica del Instituto Federal Electoral, del Instituto Electoral y de Participación Ciudadana de Coahuila, del Consejo Estatal Electoral de San Luis Potosí y de la empresa venezolana Smartmatic.

Por ser esta una experiencia pionera que permitió generar un espacio para el intercambio de puntos de vista entre especialistas en materia electoral, científica y tecnológica, se consideró importante dejar constancia de este Simposio. De tal manera que la presente memoria se pone a disposición de los ciudadanos interesados en la innovación tecnológica aplicada a los procesos electorales.

Esta publicación integra tres ponencias magistrales y 15 ponencias representativas de los temas tratados en las mesas de trabajo y, los modelos de urnas electrónicas dados a conocer durante el desarrollo de este evento.

Con este Simposio la Comisión de Organización y Geografía Electoral del Instituto Electoral del Distrito Federal buscó aportar al debate y al análisis de las implicaciones sociales, jurídicas, políticas y tecnológicas de la incorporación de urnas electrónicas a los sistemas electorales del siglo XXI.

María Elena Homs Tirado
Consejera electoral y presidenta de la Comisión de Organización y Geografía Electoral del IEDF
Noviembre de 2005

MAGISTRALES

MARCO JURÍDICO PARA LA IMPLANTACIÓN DE LAS URNAS ELECTRÓNICAS

Dr. Jordi Barrat i Esteve
Observatorio del Voto Electrónico de la Universidad de León, España

Licenciado en Derecho por la Universidad de Navarra (España) y doctor en Derecho por la Universidad de León (España), profesor titular de la Universidad de Derecho Constitucional en la Universitat Rovira i Virgili (Cataluña, España). Asimismo es integrante del Observatorio del Voto Electrónico de la Universidad de León (España) y del eDemocracy Center de la Université de Genève (Suiza).

RESUMEN

La comunicación aborda los requisitos legales que deberían cumplir los sistemas de voto electrónico consistentes en boletas ópticas y computadoras operando en modo local, es decir, en entornos de votación controlados y sin transmisión remota de los datos. Se analizan, entre otros, la verificabilidad de los resultados, las medidas necesarias para compensar la brecha digital y las garantías relativas, de forma estricta, al momento de la votación (entre otras, igualdad de votantes y candidaturas, secreto y respeto a las tradiciones electorales de cada país).

INTRODUCCIÓN

Era lógico prever que las nuevas tecnologías terminarían incidiendo en los ámbitos electorales ya que son herramientas con tal capacidad de penetración que pocos espacios, si alguno, pueden permanecer ajenos. Es por ello que, desde hace unos años, existe un creciente interés por la posibilidad de realizar votaciones vinculantes de forma enteramente electrónica. Los problemas hallados en Estados Unidos durante las últimas elecciones presidenciales aceleraron, por otra parte, un proceso que ya venía impulsándose desde diversos sectores.

Hasta ahora los esfuerzos se han centrado en el desarrollo tecnológico, pero, una vez alcanzada cierta madurez, es hora de que otras especialidades científicas aporten sus conocimientos para que la implantación del voto electrónico pueda ser efectiva. Debe advertirse, en este sentido, que toda innovación técnica tiene que ir acompañada de estudios sociales –politológicos, jurídicos, etcétera– ya que de lo contrario equivaldría a una aplicación precipitada y a un seguro fracaso.

Dentro de esta segunda fase, es preciso, como mínimo, desarrollar los tres siguientes apartados: establecer una tipología precisa de las modalidades de votación electrónica, tomar en consideración la oportunidad de introducir estos procedimientos destacando las ventajas e inconvenientes genéricos que pueden aportar y, en tercer lugar, analizar las garantías y requisitos legales que deberían reunir. El presente trabajo aborda este último tema mediante el análisis de algunos ámbitos especialmente problemáticos como el momento de la votación, la superación de la brecha digital o los mecanismos de verificación de los resultados.[1] Cabe señalar que su campo de estudio se restringe a dos de los tipos más importantes de votaciones electrónicas: las boletas ópticas y las computadoras que operan en entornos controlados y en modo local.

1. Votación

La votación constituye el momento culminante de todo el proceso electoral y, al igual que en los sistemas tradicionales, debe ejercerse de modo libre, igual, secreto y universal. Habida cuenta que cada uno de estos rasgos genera una serie de consecuencias concretas en la implementa-

[1] Para los dos primeros apartados, cfr. Jordi Barrat i Esteve (2004) "Tipología de urnas electrónicas. Su necesidad y justificación" en AA. VV. *Cap a quina societat del coneixement?*, II Congrés Online de l'Observatori de la Cibersocietat, *www.cibersociedad.net/congres2004/index_ca.html* (15 de octubre de 2004).

ción del voto electrónico, dedicaremos los próximos apartados a analizar algunas de ellas.[2]

Así, por ejemplo, un sufragio libre comporta, como mínimo, las siguientes cuatro condiciones: *a)* información previa suficiente e imparcial, *b)* ausencia de cualquier tipo de coacción, c) adaptación a la cultura y tradición electoral de cada territorio y *d)* admisión de votos en blanco y nulos.

En relación con la primera exigencia, es sabido que toda la información oficial que se ofrezca debe ser imparcial, es decir, no puede beneficiar a ninguna opción. Se prohíben asimismo todo tipo de reclamos políticos en las inmediaciones de la casilla. Si aplicamos estas características a los sistemas electrónicos, se advierte rápidamente como la polivalencia de las nuevas tecnologías, si bien es un valor positivo, también encierra algunos peligros ya que las urnas electrónicas podrían ofrecer, de múltiples maneras, información partidista. En este sentido, la recomendación ya citada del Consejo de Europa señala, por ejemplo, que: "*the electronic ballot by which an electronic vote is cast shall be free from any information about voting options, other than that strictly required for casting the vote. The e-voting system shall avoid the display of other messages that may influence the voters' choice*".[3]

Tal hipótesis puede darse con relativa facilidad en caso de las pantallas táctiles ya que permitiría emitir, de forma continua o esporádica, datos no admisibles como, por ejemplo, el slogan de un partido. También podría suceder en el caso de las boletas ópticas ya que, al menos en el sistema Demotek, el elector puede verificar que su boleta es la correcta mediante un dispositivo de luz ultravioleta y sería plausible que tal elemento, además de indicar el partido político al que corresponde la boleta, añadiera

[2] Una recopilación exhaustiva de todos los requisitos puede hallarse, por ejemplo, en la Recomendación aprobada por el Consejo de Europa en septiembre de 2004 o en el reglamento técnico aprobado por el Ministerio Francés del Interior, de la Seguridad Interior y de las Libertades Locales el 17 de noviembre de 2003: *-www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/02_Recommendation/Rec(2004)11E_rec_adopted.asp#TopOfPage* (15 de octubre de 2004). *-www.interieur.gouv.fr/rubriques/b/b3_elections/b31_actualites/2003_07_04_machines_voter/mav2.pdf* (11 de junio de 2004).

[3] Recomendación aprobada por el Consejo de Europa en septiembre de 2004, numeral 48.

algún dato más.[4] Es necesario, en definitiva, que los fabricantes de estos aparatos excluyan todo tipo de información no autorizada y que los elementos utilizados superen el correspondiente proceso de acreditación.

En relación con el segundo apartado, es decir, la necesidad de evitar coacciones, los dos sistemas analizados no presentan más problemas que los ya existentes ya que el elector sigue acudiendo a una casilla oficial y puede habilitarse, como en el caso mexicano, un lugar obligatorio para emitir el voto de forma reservada. La presencia de una posible coacción cobraría sentido si se tratara de entornos no controlados, pero no es el caso.

Por último, todo sistema de voto electrónico debe respetar las peculiaridades de cada país ya que, más allá de ciertos requisitos democráticos básicos, pueden existir tradiciones electorales que merecen ser conservadas por las nuevas tecnologías. Michael Remmert se refiere, por ejemplo, a los casos en los que *"the electoral system allows voters to change a previously cast vote on election day ('advanced preliminary voting') [o cuando] a judicial authority is authorised by law to ascertain by whom, where and by what means any ballot was cast"*.[5]

Teniendo esto presente, cabe abordar ahora la posible admisión de votos en blanco y nulos. Si bien los primeros pueden fácilmente incluirse mediante la adición de una nueva opción tanto en las boletas ópticas como en las pantallas táctiles, los segundos son más problemáticos ya que muchos sistemas electrónicos pretenden su erradicación. Un voto nulo es contemplado como un error del ciudadano y, si bien en los sistemas tradicionales de votación no puede evitarse, los electrónicos cuentan con mecanismos suficientes para guiar al elector y garantizar una votación correcta en favor de alguna de las opciones existentes.

---

[4] Cfr. Jordi Barrat i Esteve, Josep Maria Reniu i Vilamala (2004) *Informe de las experiencias de voto electrónico empleadas en las elecciones catalanas de noviembre 2003*, León / Barcelona (España), Universidad de León – OVE / Universitat de Barcelona, apartado 5, figura 6, *www3.unileon.es/dp/aco/area/jordi/treballs/evot/cat03.pdf*

[5] Michael Remmert (2003) Developing a common framework for e-voting in Europe: The Council of Europe's draft recommendation on the legal, operational and technical aspects of e-voting, ACEEEO (Association of Central and Estearn European Election Officials), Conferencia Anual / Londres, octubre 2003, lám. 13. *www.coe.int/t/e/integrated%5projects/democracy/02%5Activities/02%5Fe%2Dvoting/04%5Background%5Fdocuments/07presentation MR.asp#TopOfPage* (17 de agosto de 2004).

No suele considerarse, sin embargo, la posibilidad de que el ciudadano haya emitido consciente y deliberadamente un voto inválido. Tal situación encierra un valor participativo que no debe menospreciarse al tratarse de personas que, por diversos motivos, quieren seguramente mostrar su rechazo al sistema a través de esta modalidad de votación. Si tal cosa está permitida en los sistemas tradicionales, los electrónicos no deberían impedirlo. Además, en algunos casos, el voto nulo adquiere gran significado político. Es lo que ocurre, por ejemplo, en el País Vasco donde, tras la ilegalización de Batasuna, un porcentaje apreciable de ciudadanos utilizan boletas no oficiales con esa denominación. Se trata evidentemente de un voto nulo, pero de gran contenido político y sería erróneo implantar una votación electrónica que prohibiera tal forma de expresión.

La igualdad es otro requisito fundamental ya que los sistemas democráticos se sustentan en la participación y, desde esta perspectiva, todo ciudadano debe recibir un trato idéntico. Tal principio no comporta la ausencia de diversas modalidades de votación, pero todas ellas deben estar adecuadamente justificadas. Así, puede admitirse que alguien asista a un invidente, pero tal procedimiento sería inasumible si se aplicara de forma generalizada. Por otro lado, idénticos razonamientos podrían hacerse con relación a la igualdad entre candidatos ya que también ellos deben ser tratados de forma equitativa.

En los casos de voto electrónico, la protección de la igualdad tanto de votantes como de candidaturas exige contar, como mínimo, con los siguientes elementos:

a) Mecanismos que impidan votar más de una vez a un mismo ciudadano y que garanticen que todos los electores con derecho a sufragio podrán efectivamente ejercerlo.
b) Una presentación equitativa de las formaciones políticas.
c) Medidas adecuadas que compensen la deficiente alfabetización digital de los ciudadanos.[6]

[6] cfr. Recomendación del Consejo de Europa, aprobada en septiembre de 2004, numeral 2.

El primer requisito impone trámites robustos de registro y de identificación, pero también que, una vez superados, el sistema impida la emisión de varios votos. Podría darse el caso de que, en los modelos de pantallas táctiles, el ciudadano pudiera emitir varios votos una vez que se le ha entregado la tarjeta inteligente o una vez que se ha activado la computadora. Es lo que ocurría, por ejemplo, con las máquinas de Diebold ya que, siguiendo el informe sobre su código fuente elaborado por el equipo de Avi Rubin, *"Since an adversary can make perfectly valid smartcards, the adversary could bring a stack of active cards to the voting booth. Doing so gives the adversary the ability to vote multiple times. More simply, instead of bringing multiple cards to the voting booth, the adversary could program a smartcard to ignore the voting terminal's deactivation command. Such an adversary could use one card to vote multiple times. Note here that the adversary could be a regular voter, and not necessarily an election insider"*.[7] Reflexiones similares podrían hacerse sobre la necesidad de que, una vez superado el trámite presencial de identificación, el sistema informático admita realmente a todos y cada uno de los ciudadanos legalmente habilitados para votar.

Por otro lado, las candidaturas deben mostrarse de forma neutral, sin ningún elemento que favorezca una u otra opción. Tal planteamiento no supone un problema en el caso de boletas ópticas ya que, al tratarse de papeles similares a los actuales, deberían adoptarse las garantías que ya hoy en día se ponen en práctica.

En cambio, las pantallas táctiles plantean trabas más difíciles de sortear. Así, por ejemplo, ¿en qué orden deben colocarse las candidaturas para que sea una presentación neutral? ¿Qué ocurre si, ante candidaturas numerosas, el tamaño de la pantalla no admite la inclusión de todas ellas? ¿Resultaría admisible su distribución en pantallas sucesivas? ¿Sería compatible tal solución con el principio de igualdad?

[7] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach (2004) *Analysis of an Electronic Voting System*, 2004, IEEE Symposium on Security and Privacy, p. 10. *www.avirubin.com/vote.pdf* (18 de agosto de 2004).

De forma significativa, la Recomendación del Consejo de Europa se limita a proclamar que *"there shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote,"*[8] pero no precisa cómo debe ponerse en práctica. En cambio, el reglamento francés señala que *"les noms des candidats (scrutin nominal), les listes de candidats (scrutin de liste) ou les questions posées (référendum) doivent pouvoir, pour un même scrutin, être présentés intégralement et simultanément sur la machine à voter"*.[9]

A mi entender, la exhibición simultánea es un requisito muy relevante que sólo podría obviarse en casos excepcionales y adecuadamente justificados. De todas formas, podría argumentarse que, en una sociedad con suficientes hábitos tecnológicos, el hecho de que las candidaturas estuvieran repartidas en diversos lugares no debería preocupar ya que la transición entre varias pantallas sería un acto ampliamente interiorizado por los ciudadanos. Aun así, es sabido que, incluso hallándonos ante personas con un elevado nivel de formación, los mecanismos psicológicos inconscientes cobrarían un peso quizás excesivo favoreciendo a las candidaturas mostradas en primer lugar.

Por último, el secreto exige que nadie pueda vincular un determinado voto con la persona que lo emitió. En los comicios tradicionales tal garantía se logra mediante la mezcla en urnas transparentes de las boletas opacas. En el caso de las urnas electrónicas, la solución no es tan sencilla, pero no por ello imposible. El factor clave en estos casos consiste en el conocimiento del código fuente, pero, habida cuenta que tales datos son ininteligibles para la mayoría de ciudadanos, es sumamente importante que haya una verificabilidad individual y universal del sistema, es decir, que, aun implantando un voto secreto, el elector pueda comprobar que su voto ha sido correctamente computado y que se pueda, al igual que sucede en los comicios tradicionales, verificar la rectitud del proceso en su conjunto. Analizaremos este aspecto en el apartado tercero.

[8] Recomendación del Consejo de Europa, aprobada en septiembre de 2004, numeral 47.

[9] Reglamento técnico aprobado por el Ministerio Francés del Interior, de la Seguridad Interior y de las Libertades Locales, apartado 3.3.1 al 3.3. 2 (el resaltado es mío).

2. La brecha digital

Una vez resueltas las incógnitas tecnológicas, la aplicación práctica del voto electrónico requiere sortear todavía el deficiente nivel de alfabetización digital ya que tal cosa impide que muchas personas contemplen con naturalidad estos procedimientos.

En este sentido, una implantación precipitada podría quebrar gravemente la garantía de igualdad que debe presidir cualquier elección. Se primaría la participación de aquellos ciudadanos conocedores de los nuevos hábitos digitales y se entorpecería el voto del resto. Todo ello no significa obviamente que deban rechazarse estas innovaciones, pero es necesario considerar los efectos de la estratificación digital, así como adoptar las medidas necesarias para que el proceso electoral no resulte afectado.

La brecha digital presenta diversas dimensiones a tener en cuenta. Así, por ejemplo, muchos países carecen de conexión generalizada a las nuevas tecnologías. Por otro lado, las carencias formativas provocan que, aun existiendo esos medios, su utilización arroje grandes diferencias según el segmento de población analizado. En nuestro caso, podemos obviar el primer obstáculo ya que tanto los sistemas de boletas ópticas como los de pantallas táctiles se desarrollan en entornos controlados y no precisan, por lo tanto, la utilización de conexiones particulares.

De todos modos, resulta muy importante una correcta elección de los centros de votación. Tomando como ejemplo la consulta popular "Madrid-Participa",[10] algún centro, como el situado en la sede de la Asociación de Vecinos "La Corrala", obtuvo significativamente una elevada afluencia de ciudadanos que deseaban ejercer su derecho de sufragio. No es casual que tal dinámica se genere en una asociación de vecinos y nos demuestre la importancia que puede tener el entorno asociativo de cara a reducir la brecha digital. En el caso de "La Corrala", muchos ciudadanos que, en otras circunstancias, quizás no habrían votado, vieron facilitado su acceso

[10] Cfr. Jordi Barrat i Esteve, Josep Maria Reniu i Vilamala (2004), *Democracia electrónica y participación ciudadana. Informe sociológico y jurídico de la Consulta Ciudadana "MadridParticipa"*, versión preliminar, León (España), Observatorio del Voto Electrónico (OVE) — Universidad de León, *www.madridparticipa.org/resultados/informes.htm* (20 de agosto de 2004).

a la participación democrática por el hecho de que tal evento se desarrollaba en un entorno que les garantizaba seguridad, comodidad y ayuda. Se trataba del local donde, además de estos ensayos participativos, los socios se reúnen habitualmente con ocasión de otros actos.

Este entorno familiar no debe, de todas formas, menoscabar la seriedad de la contienda electoral. Una elección oficial no podría admitir que la jornada electoral coincidiera con una celebración interna de la asociación o que el ambiente de camaradería y cordialidad provocara que el secreto de la votación brillara por su ausencia. Ambos elementos contribuyen sin duda a paliar la brecha digital, pero generan simultáneamente daños de difícil o imposible reparación. Habrá que contar, en definitiva, con la útil colaboración de entidades como la mencionada, pero también debe mantenerse una estricta separación entre sus actividades y el acto de votación en sí mismo.

Es por ello que todo proyecto de implantación del voto electrónico requiere un programa de formación y de asistencia que logre que cada ciudadano pueda acceder al sistema con plenas garantías. Se trata, en definitiva, de diseñar un plan de trabajo a mediano y largo plazo para que la introducción de estas herramientas no sorprenda a la población. El día de la votación deberán existir equipos de ayuda que puedan solventar las dudas que surjan en ese momento; pero la alfabetización que estamos proponiendo no se limita a medidas simultáneas al momento de la votación real, deberá arrancar meses antes de ese día.

Sea como sea, por muchas que fueran las medidas adoptadas, no cabe esperar una superación rápida de la brecha digital. Nos hallamos ante un problema generacional que solamente podrá eliminarse con la llegada de ciudadanos completamente familiarizados con la sociedad de la información. Si ello es así, cabe preguntarse si resulta admisible la sustitución total de los sistemas tradicionales de votación por los electrónicos. ¿Sería válida, en definitiva, la utilización exclusiva de medios electrónicos en una sociedad donde todavía se detectan deficiencias en cuanto a la alfabetización digital?

La respuesta dependerá mucho del sistema que analicemos ya que no todos requieren el mismo nivel de conocimientos. Así, por ejemplo, las

boletas ópticas parecen compatibles con niveles bajos de hábitos digitales. Habida cuenta que su gran ventaja consiste precisamente en alterar muy tenuemente el comportamiento del elector, no habría inconveniente, al menos desde la perspectiva analizada en este apartado, en su implantación generalizada.

Las pantallas táctiles constituyen un caso intermedio entre la sencillez anterior y la mayor complejidad de otros sistemas como el voto por dispositivos telefónicos. Además, la decisión a adoptar también depende tanto del tipo de pantalla como del tipo de elección. No es lo mismo un referéndum como el celebrado en Venezuela en 2004, donde solamente había dos opciones en la pantalla –sí y no–, que casos donde se presenten diversas candidaturas. Se trata de factores a tomar seriamente en consideración de tal forma que deberá evaluarse la sencillez de cada sistema y su compatibilidad con el nivel de conocimientos digitales de la población. En algunos casos habrá que disponer canales complementarios de votación en formato tradicional, pero en otros no.[11]

Por último, la habilitación de varias modalidades de votación merece un juicio positivo ya que reduce el desequilibrio social. La posibilidad de votar a través de diversos canales tanto tradicionales como electrónicos –boletas ópticas, telefonía, pantallas táctiles, Internet, etcétera– permite que cada ciudadano opte por el sistema que le resulte más cómodo. La tecnología se adapta, en definitiva a una realidad plural en la que no existe un conocimiento generalizado de estas nuevas herramientas.

3. Verificabilidad

Cabe distinguir dos tipos de verificabilidad en función de las personas que intervienen y el alcance de la operación. Mientras la individual permite que cada elector compruebe que su voto ha sido correctamente considerado, la universal afecta al conjunto del sistema, es decir, consiste en analizar el desarrollo adecuado de todo el proceso.

[11] Cfr. el ejemplo de Vandœuvre-Lès-Nancy (2004) *Juin2004: La Fin des Bulletins de Vote... Vote Electronique: Une 1ère française à Vandœuvre!*, Vandœuvre-lès-Nancy (Francia), Mairie de Vandœuvre, www.vandoeuvre.fr/mairie/pages/fr/851.htm (20 de agosto de 2004).

En relación con la primera, los dos sistemas que estamos analizando resuelven la problemática de forma distinta. En el caso de las boletas ópticas, la existencia de comprobantes en papel no solventa la cuestión ya que, aunque puede hacerse un recuento físico similar al tradicional, se trata de un recurso excepcional. El procedimiento ordinario consiste únicamente en el recuento automático.

De todos modos, podrían habilitarse mecanismos para comprobar que la boleta escogida es efectivamente la deseada. Así, por ejemplo, el sistema Demotek admite que, antes de introducir la boleta en la urna, el elector pueda consultar su contenido mediante un dispositivo electrónico dotado de un lector de luz ultravioleta.[12] Puede tratarse de un avance, pero no es suficiente ya que ese dispositivo de lectura también podría estar trucado. La única garantía real que tiene el ciudadano es la boleta que introduce en la urna, y tal como ya se ha afirmado, su uso a efectos de recuento se reduce a circunstancias excepcionales.

En el caso de las pantallas táctiles sucede lo mismo ya que los sistemas normalmente utilizados pueden incorporar algún mecanismo que ofrezca un comprobante al elector, como:

a) En el referendo venezolano de 2004, las pantallas empleadas imprimían un papel en el que figuraba la opción elegida. Tal comprobante era recogido por el votante y debía introducirse, inmediatamente después, en una urna tradicional habilitada al efecto.[13]

b) El segundo sistema, utilizado por Indra en Argentina, expide un comprobante en papel, pero no se entrega físicamente al elector. La pantalla lo imprime, lo muestra al votante y lo almacena en una urna propia.

[12] Cfr. Jordi Barrat i Esteve / Josep Maria Reniu i Vilamala (2004) *Informe de las experiencias de voto electrónico empleadas en las elecciones catalanas de noviembre 2003*, León / Barcelona (España), Universidad de León – OVE / Universitat de Barcelona, numeral 5. *www3.unileon.es/dp/aco/area/jordi/treballs/evot/cat03.pdf*

[13] Cfr. Smartmatic (2004) *Cast your vote*, Elecciones Venezuela / Infografía, Smartmatic. *www.smartmatic.com/infografia_03.htm* (20 de agosto de 2004)

Existe también la posibilidad de que el votante conserve un comprobante, pero la especificación de la opción política elegida suele estar prohibida.[14] Se podría, por lo tanto, comprobar la participación del elector, pero no el contenido del voto.

¿Son realmente suficientes estos mecanismos para asegurar una verificabilidad individual de los votos? La respuesta es negativa. Como ya hemos afirmado, estos sistemas pueden garantizar que, en las urnas en las que se introduce el comprobante en papel, existe el voto efectivamente emitido por el ciudadano, pero nada certifica sobre la fiabilidad del recuento automático. Se trata de dos ámbitos separados que pueden, en consecuencia, operar de forma diferente.

Las catas o muestreos podrían ser la solución. De esta forma, aun no existiendo un recuento manual de todas las urnas, se escogerían aleatoriamente un número representativo de ellas para comprobar la concordancia entre el escrutinio manual y el automático. Si estas auditorías arrojan un resultado plenamente positivo, cabría presumir de forma razonable que, aun no existiendo una comprobación efectiva, todas las máquinas han funcionado de forma correcta.

Se trata ya, en todo caso, de un procedimiento incluido en lo que hemos denominado verificabilidad universal ya que intenta garantizar la corrección de todo el proceso. No existe, en definitiva, un procedimiento individual de comprobación y la credibilidad del sistema debe reposar en mecanismos de carácter universal. En este sentido, la garantía más efectiva consiste en la transparencia y exhaustiva auditabilidad de los protocolos informáticos internos. Esta es realmente la única posibilidad de ofrecer sistemas completamente creíbles. Podría plantearse una apertura total del código, pero, en muchos casos, las compañías informáticas no la admiten. Aceptan comunicarlo a ciertos actores, como los administradores electorales o los representantes de los partidos políticos, pero los

[14] Cfr. Lilian Mitrou *et al.* (2002), *Legal and regulatory issues on e-voting and data protection in Europe*, E-Vote Project, p. 19, *www.instore.gr/evote/evote_end/htm/3public/d[illegible]blic/public_deliverables/d_3_4/e_vote_D_3_4_v22_20_02_02.doc* (10 de enero de 2004).

ciudadanos, incluso aquellos especializados que podrían valorarlo con fundamento, siguen ignorándolo.

La ya citada Recomendación del Consejo de Europa[15] no obliga a desvelar completamente esos datos y se contenta con su comunicación a las autoridades electorales, pero cabe preguntarse si tales medidas son suficientes. Adviértase que la administración electoral no goza en todos los países de la misma credibilidad. El procedimiento tradicional, al basarse en recuentos públicos, permite que el ciudadano confíe en el sistema en sí mismo y no en determinadas instituciones. El voto electrónico, en cambio, genera un protagonismo creciente de técnicos que desposee al ciudadano del control directo e inmediato de la corrección de la votación. Habida cuenta de que se trata de una tendencia preocupante, debe intentar paliarse y, en este sentido, sería deseable que el conocimiento del código interno de las computadoras fuera el más amplio posible.

4. Conclusiones

Los procedimientos electrónicos de votación se hallan en una fase de transición en la que, una vez comprobada la viabilidad de las soluciones tecnológicas, hace falta que las disciplinas sociales, entre ellas la jurídica, complementen el esfuerzo científico realizado hasta la fecha.

El ordenamiento jurídico juega un papel de primer orden en la incorporación armónica y no precipitada de aquellas novedades técnicas que demuestren poder mejorar el actual proceso electoral. Debe rechazarse, en este sentido, una deriva modernizadora que, ignorando las virtudes del actual modelo, pretendiera reformarlo por el mero hecho de hacerlo, es decir, por el mero hecho de darle una pátina de mayor modernidad.

Existen diversos elementos que conviene tomar en consideración ante la implantación de mecanismos electrónicos de votación. Así, todo el proceso electoral, desde la información que recibe el votante hasta el diseño de la aplicación informática, debe estar pensado para garantizar los principios vigentes. De esta forma, entre otros elementos, la informa-

[15] Recomendación del Consejo de Europa, aprobada en septiembre de 2004, numeral 24.

ción tiene que ser neutral y suficientemente detallada, la presentación de las candidaturas debe ser equitativa y habrá que prever la posibilidad del voto en blanco y del voto nulo, si tales opciones existen en los comicios tradicionales.

El voto electrónico comporta un elevado protagonismo de los técnicos que puede, llegado el caso, oscurecer la labor que actualmente desarrollan instancias ciudadanas de base, como los miembros de la mesa electoral. Hoy por hoy, la transparencia de la urna, el recuento público, la presencia de interventores o la ya mencionada Mesa constituyen factores que permiten que cualquier ciudadano pueda controlar, por sí mismo, el desarrollo y corrección de las elecciones. Con el voto electrónico, en cambio, solamente los técnicos parecen capacitados para auditar el código fuente de las aplicaciones y se hace preciso, en consecuencia, tomar las medidas adecuadas para compensar este elevado protagonismo. La utilización de código abierto y la presencia de una mesa de custodios con competencias plenas pueden ser algunas de las soluciones.

Cabe destacar, por último, la relevancia de la brecha digital. En los dos casos estudiados, la posible discriminación entre diversos ciudadanos impone la modulación del proceso y, entre otras medidas, la articulación de una intensa campaña informativa y de asistencia.

BIBLIOGRAFÍA

DUMORTIER, Jos y Mieke Loncke "Online voting: a legal perspective" en Julian Padget, Ricardo Neira, Juan Luis Díaz de León (eds.) *e-Government and e-Democracy*, (Col. "Research on Computing Science" -8), México, Distrito Federal, Instituto Politécnico Nacional, 2004, pp. 147-164.

MITROU Lilian "Constitutional and Legal Requirements for e-Voting" en AA. VV. *Votobit Proceedings & 2003/2004 eVoting Reports*, León (España), Observatorio del Voto Electrónico / Universidad de León, 2004.

RIAL, Juan, "El voto Electrónico en América Latina. Consideraciones políticas sobre su implantación" en AA. VV. *Votobit Proceedings & 2003/2004*

eVoting Reports, León (España), Observatorio del Voto Electrónico / Universidad de León, 2004.

RIERA, Andreu, Jordi Sànchez y Laia Torras, *"Internet Voting: Embracing Technology in Electoral Processes"* en Åke Gronlund, *Electronic Government: Design, Applications and Management*, Hershey (Estados Unidos) / Londres (Reino Unido), Idea, 2002, pp. 78-98.

ANÁLISIS DE UN SISTEMA DE VOTACIÓN ELECTRÓNICA[16]

Tadayoshi Cono
Adam Stubblefield
Aviel D. Rubin
Dan S. Wallach
Instituto de Seguridad de la Información de la Universidad de Johns Hopkins

Dan S: Wallach es profesor en la Universidad Rice en el Departamento de Ciencias de la Computación. Realiza investigaciones en Seguridad en Cómputo. Obtuvo su PhD en la Universidad de Princeton, donde estudió Seguridad en Java y participó en el diseño de la arquitectura de Seguridad en Java. Realizó un posgrado en la Universidad de Berkeley en donde fue miembro de la Asociación de Graduados en Ciencias de la Computación. Ha participado en varias publicaciones entre las que destacan: *Garbage Collector Memory Accounting in Language Based Systems*, y *Runtime Support for Distributed Sharing in Safe Languages, Enforcing Java Run-Time Properties Using Bytecode Rewriting, Transactional Rollback for Language-Based System.*

RESUMEN

Se realiza un análisis de seguridad del código fuente de una de las máquinas más utilizadas en el mercado, el sistema AccuVote-TS 4.3.1 de Diebold. Este sistema está escrito en C++ y fue diseñado para ejecutarse en Windows CE pero también se compila y funciona con Microsoft Windows, por lo que el código representa un sistema completo.

El análisis muestra que este sistema de votación está por debajo de los estándares mínimos de seguridad aplicables en otros contextos e identifica varios problemas que incluyen la escala de privilegios no autorizados, el uso incorrecto de la criptografía, vulnerabilidades en la red, y procesos deficientes en el desarrollo del *software*.

[16] Extracto del artículo propiedad del Institute of Electrical and Electronics Engineers (IEEE), el cual puede consultarse en la dirección: http://avirubin.com/vote/analysis/index.html

También se demuestra que los electores, sin ningún privilegio, pueden introducir votos ilimitadamente sin que sean detectados por cualquier mecanismo dentro del *software* de la terminal de votación.

1. Sistema AccuVote TS 4.3.1 de Diebold

A continuación, se describe el proceso para la creación y funcionamiento del sistema de Diebold en una elección.

1.1 Creación

Antes de una elección es necesario definir los datos que debe presentar una boleta electoral y las terminales de votación que se requieren para configurar e instalar cada casilla. Una entidad gubernamental que usa las terminales de votación de Diebold tiene una variedad de opciones en cómo distribuir las diferentes boletas. Pueden distribuirse usando medios extraíbles, tales como disquetes o tarjetas del almacenaje, o sobre una red local, el Internet, o a través de *dial-up*. El utilizar la red proporciona flexibilidad adicional al administrador de la elección para realizar cambios de última hora en las boletas.

1.2 La elección

Una vez que la terminal de votación se inicializa con las definiciones de la boleta y comienza el proceso de votación, los electores pueden depositar sus votos. Primero, el elector debe tener una tarjeta de votación, la cual es una *Memory Card* o una *Smart Card*; es decir, es una tarjeta plástica (como una tarjeta de crédito) con un chip en el que se pueden almacenar datos y, en el caso de la *Smart Card*, además se puede realizar el cómputo. Se asume que las tarjetas de votación son entregadas a los electores en el sitio de votación el día de la elección.

El elector toma la tarjeta de votación y la inserta en un lector de *Smart Card*, el cual está unido a la terminal de votación. El lector de *Smart Card* verifica que sea una tarjeta de votación y, si es así presenta al elector una boleta en la pantalla de la terminal. La boleta real que verá el elector puede desplegar el nombre del candidato o el logotipo del partido político de su preferencia, que está codificado en la tarjeta de votación; sin

embargo, si en la boleta no se incluye o no se puede encontrar dichos datos, se le da al elector una boleta no partidista. Tales boletas partido-específicas se utilizan, por ejemplo, en elecciones primarias.

En ese momento el elector interactúa con la terminal de votación, toca las cajas apropiadas en la pantalla para seleccionar a sus candidatos. Los auriculares y los teclados numéricos permanecen disponibles para que los electores con discapacidad visual interactúen con la terminal en privado. Antes de que las boletas queden registradas en el sistema se da al elector la oportunidad de repasar su o sus selecciones; si el elector confirma esto, el voto se registra en la terminal de votación y la tarjeta de votación queda "cancelada", para evitar que el elector vote otra vez con la misma tarjeta. Después de que el elector termina de emitir su voto, la terminal queda disponible para otro elector. El elector devuelve la tarjeta de votación cancelada a los funcionarios de casilla y ellos reprograman la tarjeta para el usuario siguiente.

1.3 Divulgación de los resultados

Un funcionario concluye el proceso de votación insertando en la terminal de votación la tarjeta de administrador o una tarjeta especial que se puede utilizar solamente para terminar la elección. Una vez que se detecta la tarjeta, el funcionario confirma que la votación ha finalizado. Si el funcionario lo determina se ejecuta la etapa post-electoral, es decir, los resultados de la elección se registran en una tarjeta de memoria y pueden también transmitirse electrónicamente al servidor central.

2. Conclusiones

Usando el código fuente disponible, se realizó un análisis de lo sucedido en abril de 2002 con el sistema electrónico de votación AccuVote-TS 4.3.1 de Diebold.

Se encontraron defectos de seguridad significativos, tales como:

- Los electores pueden introducir múltiples boletas sin seguimiento de auditoría
- Las funciones administrativas pueden ser realizadas por los electores

- Los hilos de ejecución utilizados por los desarrolladores de *software* son mucho mayor

De acuerdo con el análisis del ambiente de desarrollo, se determinó que este sistema no tiene un nivel apropiado de programación, ya que cuenta con pocos controles de calidad en el proceso.

Por lo anterior se concluye que este sistema de votación es inadecuado para su uso en una elección general y que cualquier sistema de votación electrónico que no cuente con comprobantes impresos de votación puede sufrir defectos similares, pese a alguna "certificación" que pueda recibir. Se sugiere que la mejor solución en los sistemas de votación es que cuenten con un "rastro de intervención" donde el sistema de votación automatizado permita imprimir un comprobante que pueda ser leído y verificado por el elector.

Actualmente, los vendedores de los sistemas electrónicos de votación afirman que sus sistemas son seguros y aún más cuando el código no está abierto. De hecho, se cree que un proceso abierto daría lugar a un desarrollo más cuidadoso ya que los científicos, ingenieros de *software*, políticos y otros que valoran su democracia pondrían atención a la calidad del *software* que se utiliza para sus elecciones. Por supuesto, el código fuente abierto no solucionaría todos los problemas de las elecciones electrónicas, sigue siendo importante verificar que las imágenes del programa binario que funcionan en la máquina correspondan al código fuente y que los compiladores usados en el código fuente no sean malévolos. Sin embargo, el código fuente abierto es un buen comienzo. Actualmente Australia utiliza un sistema de votación con el código fuente abierto.

Alternativamente los modelos de seguridad que incluyen la impresión de un comprobante en los sistemas electrónicos de votación permiten al elector ver y verificar su voto. Incluso si, por cualquier razón, las máquinas no pueden nombrar al ganador de la elección, entonces las boletas de papel se pueden contar de nuevo, mecánicamente o manualmente, para obtener los resultados de ésta. Los comprobantes impresos son requeridos en algunos estados de los Estados Unidos, y los vendedores im-

portantes de terminales de votación han declarado que incluirán dichas características siempre y cuando sus clientes lo soliciten.

El modelo donde los vendedores cuentan con código propietario para ejecutar las elecciones parece ser no confiable, y si no se cambia el proceso de diseñar los sistemas de votación no se tendrá la confianza que los resultados de la elección reflejen la voluntad del electorado. Finalmente, se deben tener sistemas electorales robustos y bien diseñados para preservar la base de la democracia.

Apuntes para el análisis sociopolítico del voto electrónico

Josep María Reniu I Vilamala
Departamento de Derecho Constitucional y Ciencia Política
Universidad de Barcelona

Doctor en Ciencia Política y de la Administración, y profesor lector de Ciencia Política en la Universidad de Barcelona. Asimismo, es miembro del Observatorio de Voto Electrónico (OVE) de la Universidad de León; ha realizado diferentes reportes sobre la aplicación de procedimientos de voto electrónico en consultas ciudadanas y pruebas piloto en procesos electorales.

RESUMEN

Los diferentes estudios sobre los procesos de voto electrónico presentan todos una misma deficiencia: la ausencia de una vertiente sociopolítica. En aras de incorporar dicha dimensión en los procesos de diseño y análisis de las prácticas de voto electrónico se presentan algunas de las principales variables a abordar desde ese tipo de análisis. La principal aportación se halla en el estudio comparado de los diversos mecanismos de voto electrónico, donde se hace la diferencia entre voto remoto (mediante Internet o telefonía celular) y voto electrónico presencial (a través de urnas electrónicas).

INTRODUCCIÓN

La incorporación de elementos tecnológicos en los procedimientos tradicionales de votación plantea algunos retos de suma importancia, y no sólo de índole jurídica y/o tecnológica. Si bien en algunos casos los sistemas de votación electrónica son capaces de garantizar la no vulneración de los derechos básicos de los electores, lo cierto es que la introducción del voto electrónico pone sobre la mesa elementos clave en el debate sociopolítico.

Es nuestra intención presentar algunos apuntes de cuestiones a considerar en la elaboración de análisis sociopolíticos del voto electrónico. No pretendemos realizar un listado exhaustivo de todas las variables que intervienen en dicho proceso, desde la óptica sociopolítica, pero sí reflejar aquellas con una mayor importancia. En este sentido el discurso discurre por un doble cauce: por un lado presentamos los diferentes elementos en un plano teórico para, posteriormente, discutir el alcance de los mismos a partir de datos obtenidos en las experiencias acerca de los distintos sistemas de voto electrónico desarrollados en España.

Tres son nuestros principales centros de interés: la brecha digital y su impacto en la posibilidad de implementar procesos de votación electrónica; la predisposición de los ciudadanos a la utilización de las Nuevas Tecnologías de la Información y las Comunicaciones (NTIC) en los procesos de toma de decisiones públicas y, las percepciones de los ciudadanos ante la realización de pruebas piloto de votación electrónica. Finalmente ello habrá de permitirnos evaluar, desde la óptica de estas tres variables, la versatilidad que ofrecen las diferentes modalidades de voto electrónico, con especial atención a la utilización de las urnas electrónicas.

1. La brecha digital

Es ya un lugar común en la literatura sobre democracia electrónica la constatación de la existencia de diferentes grados de aceptación y de utilización de los sistemas de voto electrónico entre los grupos poblacionales con acceso a las tecnologías y los que no cuentan dicha posibilidad. El utilizar cierta tecnología, como por ejemplo el acceso a la red, requiere además de recursos económicos y de un cierto grado de conocimientos básicos, la existencia de una infraestructura adecuada. El fomento y el uso de la tecnología son por lo tanto desiguales: es lo que a grandes rasgos denominamos "brecha digital".

De forma concreta, podemos interpretar esta fractura en función de dos grandes dimensiones. Por un lado, existe una división geográfica a nivel mundial, donde se constata un acceso desigual a la tecnología según los diferentes países. A partir del Índice de Consecución Tecnológica (ICT)

del Programa de las Naciones Unidas para el Desarrollo (PNUD), se deriva la existencia de cuatro grupos de países (véase tabla 1).

Tabla 1

Grupos de países según su ICT		
Tipo de países	**Ejemplos**	**Características**
Líderes ICT > 0,5	Finlandia, Estados Unidos, Japón, Francia.	Países líderes en innovación y divulgación tecnológica.
Líderes potenciales 0,35 < ICT < 0,5	España, Bulgaria, Argentina, México.	Fuertes inversiones pero carencia de innovación. Divulgación creciente.
Adaptadores dinámicos 0,2 < ICT < 0,34	Uruguay, Tailandia, Brasil, China.	Dinamismo en el uso de la tecnología, pero aún lenta divulgación.
Marginados ICT < 0,2	Pakistán, Sudán, Nepal, Mozambique.	Divulgación y fomento del uso de las tecnologías muy insuficientes.

Fuente: PNUD, 2001. Elaboración propia. [http://hdr.undp.org/reports/global/2001/en/, 10 de agosto de 2004.

Los datos muestran claramente la existencia de una marcada diferencia entre aquellos países con grandes niveles de inversión y fomento de la tecnología y aquellos donde ni tan solo las consideradas "viejas" tecnologías (teléfono o electricidad) llegan al conjunto de la población. De hecho volvemos a encontrar en gran medida la clásica división Norte-Sur, según la cual los países más ricos aventajan a los más pobres, con una situación intermedia para aquellos que se encuentran en vías de desarrollo. Puede hablarse así de la existencia de una división digital en una dimensión geográfica.

En este sentido, independientemente de otras consideraciones políticas, este fenómeno puede afectar a las votaciones electrónicas remotas desmitificando la idea que éstas permitirían a los electores emitir su voto desde cualquier punto del planeta. El requisito de la movilidad ha de interpretarse por tanto en términos muy relativos.

Pero por otro lado, en el interior de los países la brecha digital se manifiesta en una segunda dimensión, de tipo social. Tomando como referencia los países occidentales desarrollados y democráticos, en especial España, se observa como algunos segmentos de la población pueden quedar excluidos de las NTIC en función de características como los niveles de renta,

estudios o edad. En el caso concreto de Cataluña, los estudios sociológicos realizados apuntan que el perfil del ciudadano afectado por la brecha digital es el de la mujer mayor de 55 años; ama de casa, desempleada o jubilada; sin estudios o con un bajo nivel de los mismos, así como un bajo nivel de ingresos mensuales. Así, por oposición, los hombres, jóvenes, con nivel educativo y de ingreso elevados serían los ciudadanos con un mayor acceso a las NTIC.

Los datos ofrecidos por el estudio *Actituds envers la implantació del vot electrònic*[17] apoyan dichos argumentos. En lo que respecta al porcentaje de personas que accede a la red según su sexo, da como resultado una diferencia sustancial en el acceso a la red entre hombres y mujeres. Igualmente claros son los datos relativos al uso de Internet según las franjas de edad: la casi totalidad de los jóvenes entre los 15 y los 24 años accede o ha accedido a la red. Por otro lado, menos de 9% de los mayores de 55 años declara usar o haber usado Internet. No obstante, aún es más clara y evidente la brecha en lo que al nivel formativo de los ciudadanos se refiere, siendo que sólo a partir de un nivel de estudios secundarios se constata el uso generalizado de Internet.

Si a estas características le agregamos, finalmente, la diferenciación en el uso de Internet según los ingresos mensuales familiares netos, el panorama que obtenemos refuerza claramente la existencia de una brecha digital de índole social cuya superación se presume altamente difícil. Al igual que sucedía con los datos relativos al nivel educativo, los niveles de renta establecen claramente una frontera en la que podemos situar la brecha digital en la Cataluña (y por ende España) de inicios del nuevo milenio: los 1 200 € netos mensuales (el equivalente a unos 16 mil pesos mexicanos, aproximadamente).

Si bien a menudo se argumenta que la llegada de las NTIC al conjunto de los ciudadanos es lenta pero progresiva, lo cierto es que las encuestas y los estudios realizados por diferentes fuentes ponen de relieve que una parte considerable de la población se mantiene al margen de las NTIC. En

[17] Fundació Jaume Bofill, *Actituds envers la implantació del vot electrònic*, Barcelona, España, mayo de 2004.

relación con el voto electrónico dicha realidad implica que algunos ciudadanos tendrían más facilidad que otros a la hora de utilizar cualquier mecanismo electrónico para la emisión de su voto. Dichas diferencias aún serían mayores si el sistema utilizado fuera el voto remoto, habida cuenta de la precondición que supone la posesión de un ordenador y/o el acceso a la red.

En resumen, vemos así que las variables como el nivel de estudios o de ingresos nos permiten identificar con claridad los límites de la brecha digital/social: todo parece indicar que los grupos sociales con más acceso a las NTIC son al mismo tiempo los que presentan mayores niveles educativos y económicos, así como una mayor tendencia a participar electoralmente. De tal suerte que es altamente probable que la opción por mecanismos de votación basados en el acceso a Internet no sólo no elimine las diferencias en términos de participación electoral entre unos y otros grupos, sino que incluso las acentúe.

En definitiva, se puede afirmar que son necesarios unos incentivos y una predisposición, además de un *status socio-económico* determinado para votar, que el acceso a las NTIC no aporta por sí mismo. Si este razonamiento es cierto, con la implementación de mecanismos de voto remoto se estaría facilitando la participación a aquellos segmentos de población que ya disponen de recursos suficientes (mayores niveles de ingresos o educativos) y, en sentido contrario, se ampliarían los inconvenientes para aquellos ciudadanos para los cuales la decisión respecto del voto y su contenido requiere un mayor esfuerzo en todos los sentidos.

2. La utilización de las NTIC

En el conjunto de estudios sociológicos realizados en Cataluña y España, casi nadie pone en duda las ventajas que aportan las NTIC, subrayan en especial su utilidad, entendida como aumento de capacidad, eficacia, rapidez e inmediatez (véase tabla 2).

Tabla 2

Ventajas e inconvenientes de las NTIC	
Ventajas	**Inconvenientes**
Utilidad / inmediatez	Poca fiabilidad
Ahorro de tiempo	Poca esperanza de vida
Información	Complejidad / dificultad de uso
Comunicación	Poco humano / Impersonal
	Poca seguridad

Como principales inconvenientes de las NTIC, la mayoría de los estudios coinciden en destacar la poca fiabilidad, la corta esperanza de vida de los aparatos, la cada vez mayor complejidad y en consecuencia dificultad en el uso de los mismos, y también se menciona su "frialdad": la impersonalidad o poca humanidad en una relación creciente de dependencia respecto de las máquinas. Así, frente al interés y el uso de las NTIC, aparecen cuatro perfiles sociológicos claramente diferenciados:

El primero está formado por los jóvenes que han crecido con las NTIC, y que son éstas parte importante de su vida cotidiana, y a los que podemos denominar *usuarios naturales*. Utilizan las NTIC de una manera natural, sin esfuerzo, tanto como medio de comunicación así como fuente de información.

En segundo lugar encontramos a los "conversos", mayoritariamente personas de mediana edad (30-50 años), interesadas de forma pragmática en las NTIC a nivel de simple usuario casual. Si bien han oído acerca de los problemas de seguridad y otras dificultades, por lo que aún no tienen en las NTIC una confianza plena, creen no obstante que son elementos circunstanciales debidos a la novedad y, a menudo, tienen una mayor confianza en el sistema en general.

Un tercer grupo son los "atecnológicos", formado por la gente de más edad, que demuestra un interés escaso o nulo en las NTIC, sobre las que no tiene capacidad alguna. Se siente en general lejos de las NTIC, se autoexcluye al no sentirse atraído en absoluto por las mismas. No obstante, no encuentra pernicioso si las utilizan los demás, con lo que su afirmación más habitual es: "Esto es cosa de jóvenes, no está hecho para mí".

Finalmente, encontramos al grupo de "expertos" que, o por cuestiones laborales o por vocación, son conocedores del mundo tecnológico en general y de Internet en particular. Este grupo es una minoría que manifiesta un gran interés por las NTIC, pero que paradójicamente es el grupo más reticente a su utilización en el ámbito electoral.

No obstante dichas diferencias, los ciudadanos creen que el sistema de voto tradicional, presencial en los colegios electorales mediante una papeleta es fácil, útil y fiable. Así las papeletas son fácilmente identificables y sólo es necesario depositarlas en un sobre y, posteriormente, en la urna con lo que es innecesario cualquier conocimiento técnico previo de carácter específico. La fiabilidad se garantiza con la presencia, en las mesas electorales, de un presidente, vocales e interventores, y sobre todo por la existencia física de las propias papeletas que pueden ser contadas y recontadas tantas veces como sea necesario. Además, y de suma importancia como veremos posteriormente, señalan que es un acto festivo, participativo y/o reivindicativo hasta el punto que a menudo se pone un especial énfasis en el carácter *litúrgico* de la votación. Así una de las frases más emblemáticas es la que hace referencia a las elecciones como "la fiesta cívica de la democracia", en la que la interacción humana es un factor muy significativo.

Más allá de las argumentaciones discursivas, en el estudio referenciado sobre Cataluña se estableció, a partir de las valoraciones de una encuesta, un comparativo respecto a los diferentes sistemas de voto electrónico, en una escala de 0 a 10 entre distintas características relativas a los diferentes sistemas de voto electrónico (véase tabla 3).

Tabla 3

Valoración comparativa de los sistemas de voto electrónico		
	Voto remoto (Internet + SMS)	**Urna electrónica (pantalla táctil + lector óptico)**
Privacidad	5.6	6.0
Comodidad	8.0	6.0
Ahorro	6.6	6.7
Seguridad	4.5	6.3
Facilidad	6.1	6.3
Precisión	7.7	7.5
Universalidad	5.4	6.6
Media global	6.3	6.5

Como puede observarse las únicas ventajas comparativas de los sistemas de voto remoto son la comodidad y la precisión, aunque en este último la diferencia con respecto a las urnas electrónicas es mínima. Si bien éstas obtienen puntuaciones significativas en la práctica totalidad de ítems valorados, lo cierto es que el soporte material –como el papel– sigue siendo un elemento central para conferir seguridad al sistema adoptado. Se entiende así que dicho soporte permite recurrir a él frente a dudas o problemas, con lo que se convierte en una especie de *salvaguardia* de la pureza del proceso. Aparece en este sentido lo que en alguna ocasión hemos dado en denominar *tecnolofobia*, o el miedo a la tecnología en tanto que, si exceptuamos las urnas electrónicas basadas en la lectura óptica de papeletas, no se cuenta con ninguna *prueba* material que confirme el voto depositado.[18] No obstante lo dicho, los datos de la tabla 3 muestran que, de los dos grandes sistemas de voto electrónico, el más aceptado es el de urnas electrónicas ubicadas en los colegios electorales, en especial por ser el sistema más similar al actual. En este caso se puede mantener el ambiente festivo, *litúrgico*, del día de las elecciones; los resultados se pueden

[18] Utilizamos dicho concepto por primera vez en la conferencia magistral dictada en el Instituto Electoral del Distrito Federal el 23 de julio de 2004 con el título: "Democracia electrónica y participación ciudadana. El ejemplo de la Consulta Ciudadana 'MadridParticipa'".

conocer una vez cerrados los colegios electorales (recuento instantáneo); más allá de las garantías tecnológicas del proceso de los votos.

3. La percepción en el uso de las NTIC

Hasta aquí hemos visto, de manera somera, algunos argumentos referidos a la brecha digital en su vertiente social así como la forma en que se posicionan los ciudadanos en Cataluña frente a la utilización de las NTIC. Nuestro interés ahora es mostrar cuáles han sido las percepciones de los ciudadanos cuando han *usado* dichas tecnologías en procesos de toma de decisiones realizadas en España.

Antes de continuar debemos señalar la ausencia de datos sociopolíticos que permitan desarrollar un análisis pormenorizado. De hecho es éste uno de los principales escollos a los que nos enfrentamos al estudiar el impacto de las NTIC en la sociedad. Son escasos aún los estudios basados en la captación de datos primarios, esto es, a partir de encuestas a los ciudadanos usuarios de dichos sistemas. Los ejemplos analizados son aquellos en los que personalmente hemos actuados como observadores –pruebas piloto en las elecciones autonómicas de Cataluña en noviembre de 2003 o la elección del rector de la Universidad del País Vasco en febrero de 2004– o como analistas –la Consulta Ciudadana "MadridParticipa". Las ventajas son dobles: por un lado haber podido estar presentes en dichos acontecimientos y, por otro, la utilización en dichos eventos de los cuatro sistemas de votación electrónica lo que nos permitirá realizar una tentativa de análisis comparado.

3.1. Las pruebas piloto en Cataluña, 2003

Las pruebas de voto electrónico se desarrollaron en el marco de las elecciones parlamentarias catalanas, celebradas de modo único, es decir, sin la existencia simultánea de elecciones de otro tipo. El censo, en el momento de la votación, era de 5 307 837 personas, y se trataba de las séptimas elecciones autonómicas (1980, 1984, 1988, 1992, 1995, 1999 y 2003), caracterizadas todas ellas por bajos índices de participación (alrededor del 60%) que confirman su carácter de elecciones de segundo nivel.

El ordenamiento electoral catalán no contempla la utilización de medios electrónicos en el proceso de emisión y recuento de los sufragios. De hecho, a nivel español, solamente existe la regulación aprobada por el Parlamento Vasco en 1998, aunque sus previsiones, que todavía no han sido puestas en práctica en unas elecciones parlamentarias, se hallan además en proceso de reforma. Todos los experimentos que se detallan a continuación tenían un carácter no vinculante y fueron debidamente autorizados por la Junta Electoral Central que hizo mucho hincapié en que los procedimientos de voto electrónico especificaran de forma muy clara su carácter complementario al sistema tradicional y la invalidez de todos los sufragios emitidos por esta vía. Se utilizaron a tal efecto tres sistemas de votación electrónica: voto remoto, bajo la responsabilidad de Scytl, y dos tipos de urnas electrónicas. Por un lado la urna electrónica de lectura óptica de papeletas de Demotek y, por el otro, las urnas electrónicas de pantalla táctil de Indra.

Como datos más relevantes en lo que a voto remoto se refiere, de un total de 23 234 electores censados (en México, Chile, Argentina, Estados Unidos y Bélgica), sólo 730 personas hicieron uso del mismo. Se trata, por tanto, de un escaso 3.14% de participación. Ahora, debe tomarse en consideración que, al tratarse de electores residentes en el extranjero, el porcentaje habitual de participación en las convocatorias ordinarias suele ser más reducido que el que se produce en las cuatro circunscripciones catalanas. En realidad, sólo 20% de estos electores suele hacer uso de su derecho de sufragio, con lo que los valores no son nada despreciables habida cuenta de su carácter experimental y por ende no vinculante. En lo que respecta a las pruebas con los dos sistemas de urnas electrónicas, éstas se llevaron a cabo en cinco pequeñas poblaciones catalanas: Canyelles, Creixell, Torres de Segre, La Fatarella y Llers, en las que se instalaron urnas de las empresas Demotek y de Indra, próximas a las urnas tradicionales.

Tabla 4

Índices de participación según voto tradicional y urnas electrónicas			
Población	**Porcentaje Voto tradicional**	**Porcentaje Urna Demotek**	**Porcentaje Urna Indra**
Canyelles	63.12	33.67	33.59
Creixell	63.42	39.62	49.70
Torres de Segre	70.97	42.08	46.39
La Fatarella	70.77	46.15	60.04
Llers	68.90	57.99	51.62

Los datos de participación de la tabla 4 indican una mayor aceptación de los sistemas de voto electrónico basados en urnas electrónicas. Si bien uno de los mejores motivos explicativos pueda hallarse en la comodidad que para el elector tiene el sistema al no requerir acciones específicas con carácter previo (i.e. la obtención de una credencial para el voto remoto) así como la coexistencia en el mismo colegio de ambos sistemas, lo cierto es que los dos modelos de urnas electrónicas son los que implican menos cambios en el comportamiento electoral del ciudadano. De estos sistemas, el desarrollado por Demotek es el más parecido al voto tradicional al no sustituir ni la urna ni la papeleta, aunque por otro lado es también el que ofrece menos versatilidad ya que únicamente se consigue acelerar el recuento, pero no descentralizarlo.

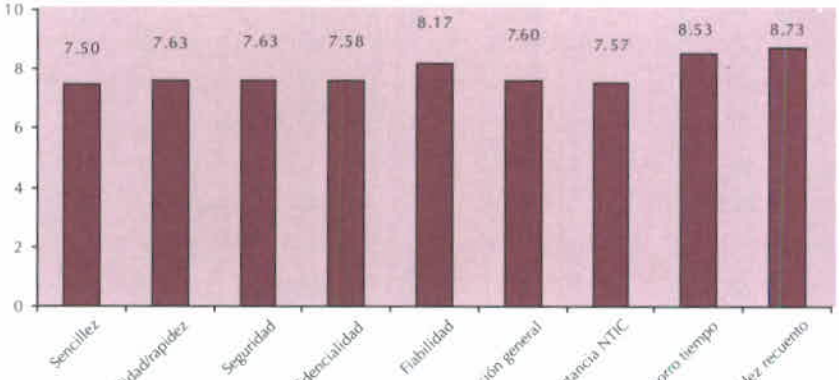
No debe olvidarse que, para el caso español, una de sus ventajas más relevantes consiste en que es compatible con la encuesta electoral de papeletas de votación que los partidos políticos españoles acostumbran a realizar durante la campaña. Aun siendo un elemento alejado de la estricta técnica informática y basado en elementos sociopolíticos, no cabe desdeñar su trascendencia habida cuenta de que son precisamente los partidos políticos y sus representantes quienes deben involucrarse en la aplicación y generalización de los sistemas de voto electrónico. No obstante, los datos de participación muestran que los electores emplearon más el sistema de pantalla táctil de Indra. Si bien ya hemos señalado la carencia de datos sociológicos al respecto, las charlas informales durante el desarrollo de las tareas de observación electoral indicaron como prin-

cipal argumento a favor de dicho sistema la facilidad en la identificación de la opción política deseada.

3.2. La elección del Rector de la Universidad del País Vasco, 2004

Una de las pocas ocasiones en que los sistemas de voto electrónico han sido utilizados de manera vinculante fue la elección del rector de la Universidad del País Vasco (UPV) por sufragio universal ponderado de la comunidad universitaria. El único sistema empleado fue la urna electrónica de Demotek en ambas rondas de votación, toda vez que en la primera ronda ninguno de los candidatos obtuvieron la mayoría absoluta de los votos ponderados. Nuestro interés se centra en los datos obtenidos por una encuesta levantada por la misma empresa, Demotek, sobre miembros de las mesas electorales y votantes (véase gráfico 1). En ella se solicitaba la valoración de diferentes aspectos del sistema de voto electrónico utilizado, valorándolos en una escala de 0 a 10.

Gráfico 1. Valoración de la urna electrónica de Demotek utilizada en las elecciones al rector de la UPV, 2004.



Los datos muestran que la valoración de los diferentes aspectos es altamente positiva, y destacan como puntos fuertes: la rapidez en el recuento (8.73 puntos), el ahorro de tiempo que supone la utilización de

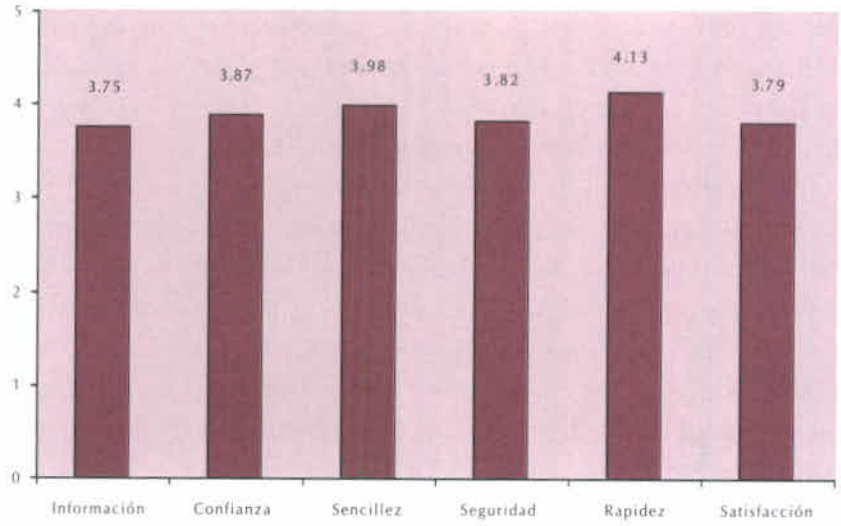
dicho sistema (8.53 puntos), así como la fiabilidad del mismo (8.17 puntos). Que sean estos tres aspectos los mejor valorados no es baladí, sino que nos reafirma en nuestro anterior comentario respecto de la utilización de urnas electrónicas: su mayor similitud con el sistema tradicional las hace más aceptables a ojos del ciudadano medio. Por otro lado es relevante que los ciudadanos pongan especial énfasis en valorar muy positivamente los principales elementos diferenciales introducidos por las NTIC: una mayor velocidad y fiabilidad en el recuento de los votos. Ello parece indicar que los principales frentes sociopolíticos en los que se podrán apoyar los programas de introducción de las NTIC en el ámbito electoral serán, precisamente, la percepción que la incorporación de la tecnología supone una mejora en el ahorro de tiempo y de recursos, a la par que otorgaran una mayor fiabilidad en el procesamiento de los datos electorales.

3.3. La Consulta Ciudadana "MadridParticipa", 2004

El último de los ejemplos en nuesta aproximación al estudio sociopolítico del voto electrónico fue la consulta ciudadana auspiciada por el Ayuntamiento de la ciudad de Madrid durante los días 28, 29 y 30 de junio. Tal y como ya hemos puesto de manifiesto, ésta ha sido la experiencia de voto electrónico con mayor relevancia en la historia española, siendo llamados a participar más de 136 mil ciudadanos del Distrito Centro de Madrid.[19] Se utilizaron dos sistemas de voto electrónico, ambos remotos: el voto a través de Internet y el voto a través de telefonía celular. En este último podía realizarse el voto a través del envío de un mensaje corto SMS o bien ejercer el voto desde terminales celulares equipadas con la tecnología JAVA.

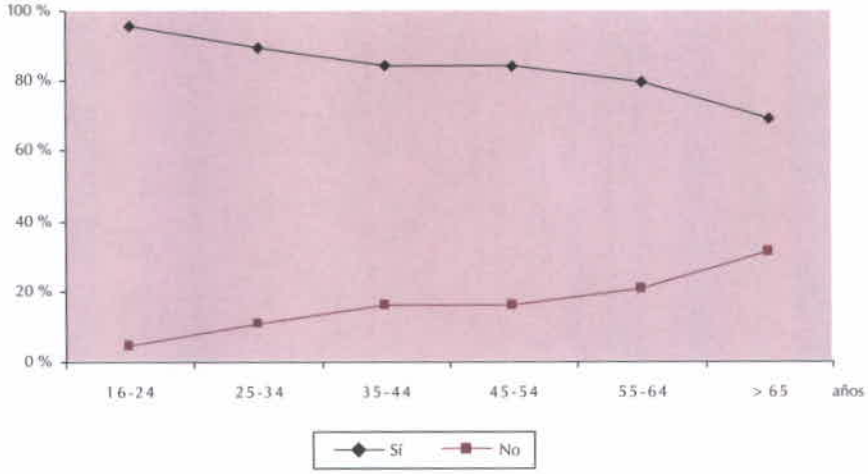
[19] Véase el informe preliminar emitido por los doctores Jordi Barrat y Josep María Reniu: *Democracia electrónica y participación ciudadana. Informe sociológico de la Consulta Ciudadana "MadridParticipa"*, julio de 2004, http://www.madridparticipa.org (22 de julio de 2004).

Gráfico 2. Valoración de los sistemas de votación; "MadridParticipa", 2004



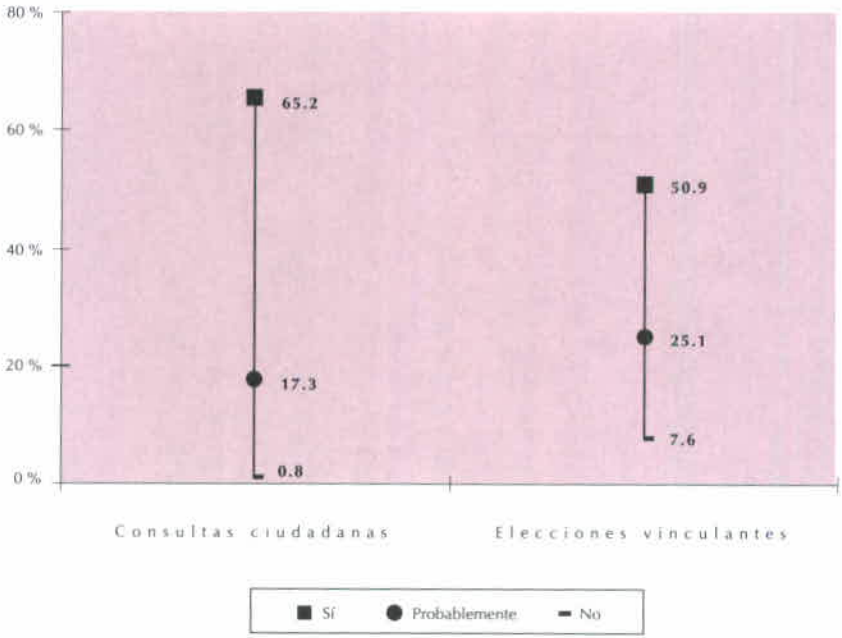
Al igual que en el estudio sociológico realizado por Demotek en las elecciones del rector de la UPV, la encuesta realizada entre los votantes de la Consulta Ciudadana "MadridParticipa" también incluyó preguntas de valoración de los sistemas de voto electrónico utilizados. En el caso de la encuesta de "MadridParticipa" se pedía a los votantes que valorasen, en una escala de 0 a 5, cuestiones relativas a la información recibida sobre el funcionamiento del sistema, la confianza que les daba dicho sistema, la sencillez, seguridad y rapidez del mismo, así como el grado de satisfacción general (véase gráfico 2). Como en el estudio anterior, también aquí se valoran muy positivamente los sistemas de voto electrónico utilizados, aunque casi exclusivamente las valoraciones se refieren al voto remoto a través de Internet. En este sentido, merece destacarse que el aspecto mejor valorado es la rapidez en la votación, con lo que éste parece convertirse en el principal valor añadido de los diferentes sistemas de voto electrónico. Otro de los intereses en nuestro análisis sociopolítico era la actitud futura de los ciudadanos o, en otras palabras, su predisposición a aceptar la generalización en el uso de las NTIC en procesos de toma de decisiones.

Gráfico 3. Predisposición hacia la generalización en el uso de las NTIC según grupos de edad.



A este respecto, el gráfico 3 corrobora nuestras afirmaciones anteriores sobre las características sociológicas de la brecha digital. Los datos indican de forma clara la existencia de una relación inversamente proporcional entre la predisposición a aceptar la generalización en el uso de las NTIC y la edad. Dicha relación parece acentuarse a partir de los 65 años, edad que en España se corresponde con el abandono de la actividad laboral. Igualmente interesante es apreciar el grado en la aceptación de dicho uso. Nos referimos a la diferenciación entre el uso de las NTIC en consultas ciudadanas como la celebrada en Madrid o en procesos electorales vinculantes (véase gráfico 4).

Gráfico 4. Predisposición al uso de NTIC según tipo de proceso



El colectivo de ciudadanos a favor de la generalización del uso de las NTIC (alrededor del 84%) muestra una tendencia bastante significativa en lo que se refiere al tipo de proceso en que dichas tecnologías se vayan a aplicar. Por un lado los datos del gráfico 4 apoyan el uso de las NTIC en procesos de consulta ciudadana, donde casi dos tercios de los votantes se manifiestan partidarios de ello (65.2%), en consonancia con las buenas valoraciones recibidas por el conjunto de la Consulta Ciudadana "Madrid-Participa". Por el otro, el uso del voto electrónico en elecciones vinculantes, los niveles de apoyo caen hasta casi 51%, y una cuarta parte de ciudadanos se manifiesta sin una decisión clara, mientras que cerca del 8% rechaza explícitamente dicha posibilidad. La interpretación de estos datos, además, debe tomar en consideración que la encuesta únicamente fue aplicada a aquellos ciudadanos que tomaron parte en la consulta ciudadana, por lo que todo parece indicar que dichos valores se verían

sensiblemente reducidos al incorporar las opiniones de los ciudadanos que no participaron en el proceso. Se constata así la presencia de un importante sesgo pro-tecnológico inducido por la voluntad de los ciudadanos por tomar parte en la Consulta. En este sentido no debe olvidarse que los ciudadanos debían, con anterioridad a su participación efectiva, obtener una credencial individual para poder emitir su voto con lo que esta "doble" movilización puede interpretarse como una predisposición previa de carácter positivo hacia todo lo que rodeó dicha experiencia.

No obstante la importancia del citado efecto, los datos socioeconómicos de que disponemos nos permiten evaluar el impacto de la brecha digital en su vertiente económica. Así en la relación que se establece entre la predisposición a aceptar la generalización en el uso de las NTIC y el nivel económico, el *corte* o la frontera donde visualizar la brecha digital se sitúa en los 1 200 € mensuales. Se confirma la tendencia en la reducción del apoyo a la generalización del uso de las NTIC al incrementarse la edad y el porcentaje de ciudadanos por debajo de los 1 200 € mensuales. Otra de las posibles explicaciones a las buenas valoraciones recibidas por la Consulta Ciudadana "MadridParticipa" es la que hace referencia al nivel de familiaridad de los ciudadanos con la base de la tecnología empleada. Efectivamente, al exceptuar al segmento de personas mayores de 65 años, se observó una evolución casi mimética entre la posesión de ordenador personal en el domicilio y la actitud pro-tecnológica. Además se constató que la posesión de ordenadores en el domicilio, y por lo tanto el grado de familiarización con las NTIC es más elevado entre los jóvenes y desciende paulatinamente al aumentar la edad del encuestado.

4. Conclusiones

Tras habernos detenido en algunas cuestiones que entiendo son indispensables en el análisis sociopolítico del voto electrónico, me parece oportuno lanzar algunas reflexiones con el objetivo de enriquecer el debate. En primer lugar hay que volver a hacer hincapié en la necesidad, desde una óptica sociopolítica, de tener como principal preocupación los problemas derivados de la brecha digital. Hemos podido observar que los datos nos indican que las líneas de esa fractura se orientan especialmente

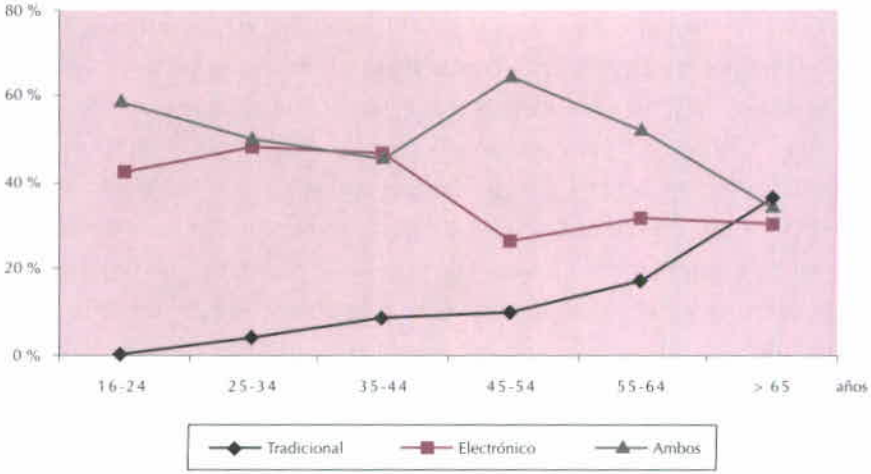
en lo relativo a nivel de instrucción y, de manera más concreta aún, al nivel económico de los ciudadanos. Ello nos lleva a reiterar la importancia no sólo de planificar la implementación de sistemas de voto electrónico sino sobre todo la urgente necesidad de conocer las opiniones y actitudes de los ciudadanos ante tales avances tecnológicos. La ausencia de estudios sociopolíticos de amplio alcance, más allá de los análisis parciales y coyunturales de que disponemos, lastra buena parte del éxito en la generalización del uso de las NTIC en los procesos de toma de decisiones políticas. Si bien el acento ha sido puesto hasta la fecha en las cuestiones tecnológico-jurídicas –sin duda de suma importancia– no es menos cierto que su puesta en práctica deberá contar con la aceptación generalizada de la población. En ese proceso he mostrado cómo la brecha digital puede operar dejando al margen a una parte más que considerable de la ciudadanía. Sin duda alguna coincido en que ningún intento de profundización democrática puede soportar el lastre de dejar en el camino a parte de sus protagonistas. Junto con ello es imprescindible también incidir en la capacitación de la ciudadanía, no sólo en términos tecnológicos vinculados a la utilización del sistema a aplicar sino sobretodo en la difusión de los mecanismos de funcionamiento con el objetivo de generalizar la percepción de seguridad y fiabilidad de los diferentes sistemas.

La segunda reflexión refiere también a uno de los lugares que no por comunes son menos evidentes: la coexistencia y complementariedad de los sistemas de voto tradicionales y electrónicos. A partir de los escasos datos sociopolíticos con que contamos se puede afirmar que los ciudadanos han valorado como muy positiva la incorporación de las NTIC a los procesos de toma de decisiones políticas. Si bien dichas valoraciones han oscilado en función del ámbito político (pruebas piloto en elecciones autonómicas, elecciones académicas vinculantes o consultas ciudadanas, por ejemplo), lo cierto es que los diferentes sistemas han obtenido siempre excelentes registros. Asimismo se han apreciado diferencias en las valoraciones de las distintas características o aspectos definitorios de cada uno de los sistemas. No obstante hay un ámbito en el que la coincidencia ciudadana es mucho mayor y que debe ser una guía para los responsables del diseño y la implementación de estos sistemas. Dicha cuestión no

es otra que el debate sobre la coexistencia entre el voto tradicional y los sistemas de voto electrónico. Aunque cada vez son menos las voces de *ciberoptimistas* que defienden la substitución total de los sistemas tradicionales por los electrónicos, también por suerte lo son sus antagonistas, los *tecnolofóbicos*. La tendencia resultante es aquella que pone de relieve la importancia de la coexistencia de ambos sistemas de votación. Las ventajas que se aducen al respecto son varias aunque todas descansan en la aconsejable introducción paulatina de los sistemas basados en las NTIC. Esta importancia del *tempo* en la generalización del uso de sistemas de voto electrónico cuenta con un amplio abanico de argumentos. Por un lado se hace mención de la necesidad de mostrar a los ciudadanos que el uso de las NTIC no supone desvirtuación alguna de los resultados "habituales" en los comicios en los que se emplea el voto tradicional. Se señala así que la coexistencia de los dos sistemas pondrá de relieve como el comportamiento electoral de los ciudadanos no varía, siendo el mismo con cualquier soporte tecnológico. Por estas mismas consideraciones se señala que ello supondrá una importante labor pedagógica, al mostrar la *bondad* de dichos sistemas.

Asimismo, la defensa de la coexistencia de ambos tipos de voto se apoya también en la capacidad de las NTIC por facilitar la incorporación al proceso democrático de una parte importante de la ciudadanía: los residentes en el extranjero. La substitución del voto por correo por una solución tecnológica basada en voto remoto es, en este sentido, uno de sus principales argumentos. En el caso mexicano la problemática no sólo se sitúa en este extremo sino que debe buscarse en la propia legislación electoral; en el sistema político español es ésta una de las opciones centrales en los estudios sobre la posible utilización del voto electrónico.

Gráfico 5. Opiniones de los ciudadanos ante la coexistencia de los sistemas de voto

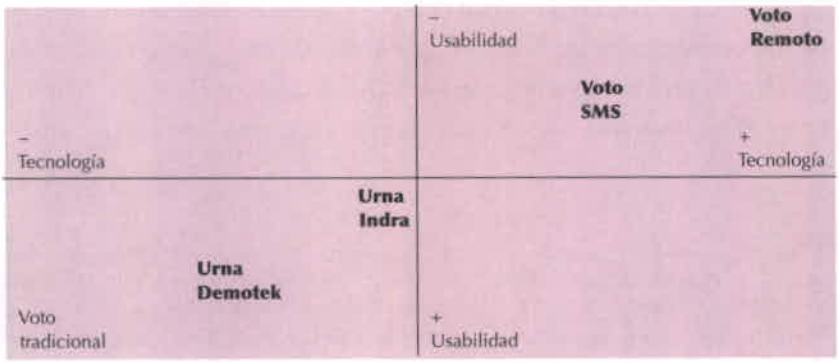


En todo caso, uno de los argumentos que mejor apoyan la necesidad de coexistencia de ambos tipos de voto lo aportan los mismos ciudadanos. Como ejemplo de ello el gráfico 5 muestra las opiniones de los participantes en la Consulta Ciudadana "MadridParticipa". Más allá de los valores concretos el gráfico pone de relieve dos grandes tendencias: por un lado el voto electrónico no merece aún la suficiente confianza como para obtener los mejores índices de predilección, de forma que se confirma que la opción preferida es la coexistencia de ambos sistemas de voto, tradicional y electrónico. Pero por otro lado no hay que minusvalorar el dato según el cual a medida que crece la edad del ciudadano crece también su predilección por el mantenimiento del actual sistema de voto tradicional. No sólo se refuerza dicho argumento de la complementariedad de los sistemas, sino que además los datos nos permiten reforzar la identificación de los grupos de mayor edad como principales destinatarios de las acciones, formación e información necesarias para garantizar el éxito de la generalización de los sistemas de voto electrónico.

Finalmente, en tercer lugar, a la luz de las experiencias analizadas se puede perfilar un esquema de clasificación de los sistemas de voto

electrónico en función de dos de las principales variables para su implementación: grado de evolución tecnológico y facilidad de uso.[20] Nos encontramos así con una disposición muy similar a un continuo evolutivo (véase gráfico 6), en el que la solución más *sencilla* tecnológicamente así como más fácil para el ciudadano es la urna electrónica diseñada por Demotek. Aunque ello habría de suponer un grado de mayor aceptación ciudadana, habida cuenta la escasa modificación del sistema de voto tradicional, lo cierto es que el avance tecnológico se encuentra en la frontera de la calificación misma de NTIC. En el otro extremo del continuo se sitúa el voto remoto como ejemplo de la más avanzada tecnología de voto electrónico en tanto que introduce la virtualidad en el proceso de votación. La posibilidad del *voto en pijama* como expresión gráfica de la desaparición de los condicionantes de tiempo y espacio para la participación es, al mismo tiempo, fuente de ventajas e inconvenientes.

Gráfico 6. Una clasificación de los sistemas de voto electrónico



[20] Somos concientes que la tipología puede construirse a partir de otras variables, ya sea adicionándolas a las dos propuestas o sustituyéndolas por otras. En cualquier caso recuérdese que son sólo reflexiones cuya finalidad es, precisamente, que formen parte del debate existente.

Entre ambos extremos encontramos dos soluciones que, a primera vista, revisten altas probabilidades de éxito social: el voto a través de telefonía celular –básicamente mediante el envío de mensajes cortos SMS– y la urna electrónica tipo Indra. De estos dos sistemas el primero cuenta como ventaja principal el alto grado de difusión que tienen los teléfonos celulares entre la ciudadanía.[21] Desde el punto de vista de sus defensores ello puede operar como un elemento de *rotura* de la brecha digital, habida cuenta de su popularidad y relativa facilidad en el uso del mismo. Por otro lado, no obstante, permanecen algunas sombras sobre la utilización de los teléfonos celulares, como por ejemplo el coste del ejercicio del voto[22] o la escasa relevancia social otorgada a dicho sistema como vehículo de expresión política.[23]

El último de los sistemas, la urna electrónica tipo Indra, es el que parece reunir mayores posibilidades de éxito a tenor de lo analizado hasta ahora. En primer lugar, dicha solución tecnológica se caracteriza por un nivel más que aceptable de facilidad de uso, gracias en gran medida a su suporte visual y a su similitud con los cajeros automáticos. En segundo lugar, no supone una ruptura con el proceso participativo tradicional, toda vez que es necesaria la presencia del ciudadano en el colegio electoral y, por lo tanto, se mantiene el carácter *litúrgico* del acto electoral. En tercer lugar, el componente tecnológico permite su rápida adecuación a todo

[21] Sin ir más lejos, los datos del Instituto Nacional de Estadística (INE) indican que 9 de cada 10 ciudadanos españoles poseen un teléfono celular, mientras que sólo 4 de cada 10 poseen ordenador personal, y sólo 2.5 de cada 10 tiene acceso a Internet.

[22] En el caso de la Consulta Ciudadana "MadridParticipa" los ciudadanos que optaron por el envío de un SMS o bien votaron a través de teléfonos con soporte JAVA tuvieron que asumir el coste de la llamada correspondiente. Cada mensaje SMS tuvo un costo de 0.15€ + IVA (aproximadamente 2.1 pesos mexicanos + IVA), mientras que el costo de la descarga del programa JAVA dependía del contrato del usuario con su respectivo proveedor de telefonía. Este costo económico para el ciudadano conlleva un serio cuestionamiento a la pureza del proceso democrático, puesto que puede agudizar aún más la brecha social.

[23] El uso habitual de los mensajes SMS en todo tipo de programas televisivos así su uso generalizado como herramienta de comunicación entre los sectores sociales más jóvenes provocó, en el estudio referenciado de la Fundació Bofill, que se descalificara la posibilidad de votar vía SMS, indicando que "el celular sólo puede servir para las nominaciones de Gran Hermano (la denominación en España del programa televisivo Big Brother) pero no para votar".

tipo de consultas, cualesquiera que sean las formas de expresión del voto. Finalmente, en cuarto lugar, su implementación puede reportar un ahorro económico considerable en la infraestructura requerida para la realización de cualquier consulta electoral, amortizándose la inversión realizada en un breve plazo de tiempo.

En resumen, las diferentes experiencias realizadas hasta la fecha y los escasos datos sociopolíticos generados a partir de las mismas parecen apuntar, como principal conclusión, hacia varias direcciones: *a)* la desmitificación del recurso a las nuevas tecnologías como panacea del proceso democrático, *b)* la obligada implementación paulatina de los diferentes sistemas de voto electrónico, que deberán convivir con los sistemas de voto tradicional, y *c)* la inexcusable necesidad de llevar a cabo programas de alfabetización digital, desarrollo de infraestructuras tecnológicas y, sobre todo, continuar en los procesos de pedagogía política democrática.

Sólo a partir de una ciudadanía informada, capacitada y con acceso a las NTIC podremos enfrentar el reto de mejorar las vías tradicionales de la participación política y, al mismo tiempo, abrir nuevos espacios para que los ciudadanos sean copartícipes de las decisiones que habrán de afectarles en el gobierno de la *res pública*.

BIBLIOGRAFÍA

FUNDACIÓ JAUME BOFILL, *Actituds envers la implantació del vot electrònic*, España, 2004.

INSTITUTO NACIONAL DE ESTADÍSTICA (INE).

BARRAT, Jordi y Josep María Reniu, *Democracia electrónica y participación ciudadana. Informe sociológico de la Consulta Ciudadana "MadridParticipa"*, España, 2004.

RENIU i Vilamala, Josep María "Democracia electrónica y participación ciudadana. El ejemplo de la Consulta Ciudadana 'MadridParticipa'" (conferencia magistral presentada en el Instituto Electoral del Distrito Federal), México, 2004.

Seguridad en el uso de urnas electrónicas

Implementación del algoritmo RSA para su uso en el voto electrónico

Liliana García Ochoa
Universidad Autónoma Metropolitana (UAM)

Es ingeniera en Sistemas Computacionales y cursa la Maestría en Ciencias de la Computación en la UAM, unidad Azcapotzalco, y trabaja profesionalmente en el Banco de México.

Germán Morales Medina
UAM

Ingeniero en Electrónica, cursa la Maestría en Ciencias de la Computación en la UAM, unidad Azcapotzalco, y trabaja en la empresa Inova.

Silvia B. González Brambila
UAM

Es doctora en Ciencias de la Computación, coordinadora de la Licenciatura de Ingeniería en Computación de la UAM, unidad Azcapotzalco. Área de investigación: Razonamiento Cualitativo.

RESUMEN

Se analiza el entorno del proceso actual de votación y cómo éste puede realizarse electrónicamente mediante el uso de tecnología especializada como lo es el algoritmo RSA. Para ello se analizan los mecanismos de seguridad existentes y se hace énfasis en los aspectos de seguridad que deben observarse en el proceso de votación electrónica. Lo anterior con la finalidad de proponer como mecanismo criptográfico para el voto electrónico al RSA, considerando en su implementación la librería OpenSSL.

INTRODUCCIÓN

Alrededor del mundo se agrupan con el término de *voto electrónico* diversas alternativas para la implementación de la tecnología en mecanismos de emisión de votos como lo son las urnas electrónicas, las lectoras

automáticas, el voto por Internet, el uso de dispositivos como el celular y los asistentes personales digitales conocidos como PDAs (*Personal Digital Assistant*).

El voto electrónico es similar al tradicional pero se basa en computadoras, redes de comunicaciones electrónicas y protocolos criptográficos. Se prevé que esta forma de votación pueda llegar a ser más rápida, barata, conveniente, e incluso más segura.

El interés dentro de este campo se desarrolla rápidamente, y debido a esto, hoy podemos encontrar en Internet varios proyectos piloto documentados, entre ellos, las elecciones primarias presidenciales de Arizona Democratic Party realizadas en marzo del 2000, donde casi 50% de los votos se efectuó mediante Internet, o las elecciones de julio de 2003 en nuestro país, cuando el proyecto piloto se aplicó para conocer la identificación partidaria de los ciudadanos (http://www.eluniversal.com.mx/graficos/ife_urna/prueba_piloto.html). Aunado a lo anterior, existen diversas compañías que ofertan infraestructuras para realizar el voto electrónico, como es el caso de vote.com e Indra Sistemas, y los proyectos de estudio sobre el voto electrónico de la Unión Europea (www.eucybervote.org) y de la Fundación Nacional de Ciencia Norteamericana (www. internetpolicy.org), entre otros.

Lo expuesto nos permite vislumbrar un importante crecimiento sobre la materia, pero no se puede ocultar el hecho de que la votación electrónica aún está en sus primeras fases de desarrollo. Existen muchos aspectos por resolver en torno al tema, entre los que destacan: la seguridad, la factibilidad, la escalabilidad, los costos, los modelos de negocio, los estándares y las consideraciones legales, políticas y sociales.

Los sistemas de voto electrónico deben proporcionar garantías voto a voto sobre su confiabilidad, así como demostrar su eficiencia. Es decir, que a través del voto electrónico se garantice:

- La secrecía: que el voto sea secreto
- La unicidad e intransferibilidad: que no exista duplicidad de votos
- La autenticidad: que sólo voten los que pueden hacerlo
- La integridad: que no exista la posibilidad de manipular el voto

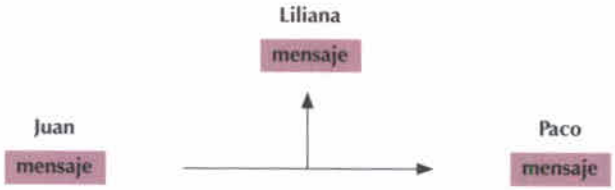
Es por ello que los sistemas que soporten el voto electrónico deberán considerar como pieza fundamental en su arquitectura mecanismos de seguridad que no sean fáciles de romper, de manera que el voto no esté expuesto a ataques o manipulaciones externas.

1. La criptografía y sus tipos

La seguridad de un sistema siempre es una mezcla de prevención, detección y respuesta. Aunque la criptografía es una parte pequeña de la seguridad de un sistema también se considera como la parte crítica[24] que permite que algunos tengan acceso a la información y otros no. El encriptamiento o ciframiento es el objetivo de la criptografía.

Veamos lo siguiente: Si dos personas (Juan y Paco) desean comunicarse, encontrarán que generalmente los canales de comunicación no son seguros porque alguien más puede recibir el mensaje (véase figura 1).

Figura 1. Esquema general de comunicación, usualmente la comunicación no es segura

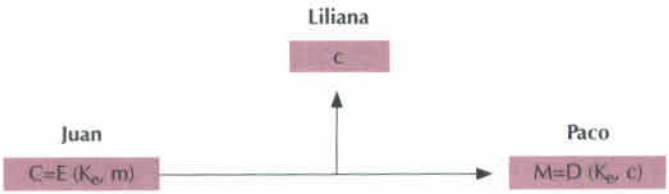


Así, cualquier mensaje que Juan envíe a Paco también será recibido por Liliana, análogamente los mensajes que envíe Paco a Juan. Para prevenir que Liliana se entrometa en la conversación de Juan y Paco se utiliza la criptografía (véase figura 2), donde Juan y Paco se ponen de acuerdo en una llave secreta K_e, normalmente a través de un canal seguro de comunicación. De tal forma que cuando Juan envíe un mensaje m, primero lo cifra usando una función de encriptamiento, $E(K_e,m)$, y entonces envía a Paco un mensaje cifrado $c = E(K_e,m)$ y cuando Paco reciba c,

[24] Ferguson, Niels, Schneier, Bruce, *Practical Cryptography*, Wiley, 2003.

lo desencripta usando una función $D(K_e,m)$ de donde obtiene el mensaje original m que Juan le envío.

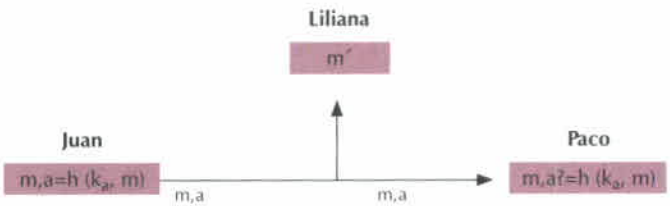
Figura 2. Esquema general de encriptamiento



El principio de Kerckhoffs[25] establece que la seguridad de un sistema depende sólo de la secrecía de la llave y no de la secrecía de los algoritmos.

Una desventaja de este esquema es que Liliana puede cambiar el mensaje de alguna forma, por lo que se utiliza la autentificación, donde se emplea una llave secreta K_a que sólo Juan y Paco conocen, de tal forma que identifique quién envío el mensaje, y en su caso, reconocer el mismo. Así, cuando se envía un mensaje m, se calcula un MAC (*Message Authentication Code*). Generalmente la autentificación se combina con un esquema de numeración que permite reconocer la secuencia de los mensajes, y el reenvío de éstos para evitar la pérdida de información.

Figura 3. Esquema general de autentificación

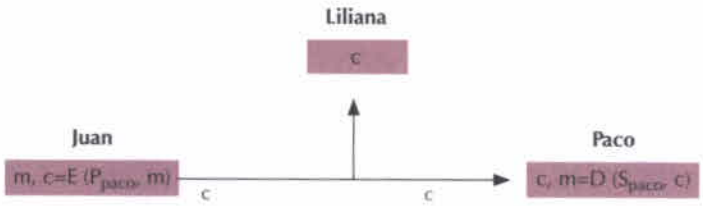


El problema que se presenta cuando dos personas comparten una llave, es el número de llaves que se requieren para que se comuniquen varias

[25] Welschenbach, Michael, *Cryptography in C and C++*, Apress, 2001.

parejas (por ejemplo, para 20 personas se requieren 190 llaves). Un esquema diferente llamado de llave pública o no simétrico, permite que Juan y Paco tengan llaves diferentes. Por ejemplo, Paco genera un par de llaves (S_{Paco}, P_{Paco}), S_{Paco} es llamada la llave secreta y P_{Paco} la llave pública. Así, cuando Juan desea enviar un mensaje a Paco busca la llave pública de Paco, Juan encripta el mensaje m utilizando P_{Paco} de donde obtiene c y envía a Paco a c. Paco utiliza su llave secreta S_{Paco} y desencripta el mensaje para obtener m (véase figura 4), donde se cumple que $D(S_{Paco}, E(P_{Paco}, m)) = m$.

Figura 4. Encriptamiento de llave pública



Las firmas digitales son el equivalente de la llave pública en los códigos de autentificación de mensajes.

La criptografía de llave pública ofrece ventajas sobre las técnicas simétricas, como son las siguientes:

- No se requiere compartir una única llave
- Firmas digitales
- Establecimiento de identidad

Se recomienda el uso de criptografía de llave pública cuando existe intercambio de llaves o firmas digitales ya que es computacionalmente costoso.[26] La criptografía de llave pública permite comunicarse en forma segura sin necesidad de establecer una llave a través de un canal seguro.

[26] Viega, John, Messier, Matt, *Secure Programming Cookbook for C and C++*, O'Reilly, 2003.

La velocidad es otro de los factores importantes en la criptografía de llave pública, ya que el más rápido de los algoritmos de criptografía pública considera varios órdenes de magnitud más lentos que los simétricos. Versiones del algoritmo RSA[27] que se basa en curvas elípticas son más eficientes pero no se recomiendan para usos de propósito general.[28] Así la criptografía de llave pública es realmente útil sólo para procesar pequeñas piezas de datos y como resultado se usa ampliamente para el intercambio de llaves y para firmas digitales.

Al utilizar la criptografía los desarrolladores frecuentemente cometen errores que tienen que ver principalmente con la forma de aplicarla, lo que resulta en un mal uso o desuso de la criptografía en las aplicaciones, volviéndolas vulnerables a diferentes ataques.[29]

2. Recomendaciones de Implementación

Cuando dentro de una aplicación se considera necesario utilizar la criptografía, distintos autores,[30 y 31] basados en su experiencia, recomiendan emplear algoritmos publicados que han sido analizados por otros criptógrafos durante varios años. La principal razón de esta recomendación es que el escribir un nuevo algoritmo criptográfico es una tarea excepcionalmente difícil que requiere un estudio profundo del campo, y usualmente la gente no confiará en él, sino hasta después de varios años de revisión y pruebas.

Otra de las grandes falacias es que al aplicar la criptografía se obtiene integridad en los datos. Si sólo se cifra un flujo de datos un atacante podría modificar su contenido, lo que quizá convertiría los datos en basura (si se asume que el atacante no conoce la llave) y tener efectos posiblemente devastadores si no se manejan adecuadamente las condiciones de error. Una solución común a esto es que cuando se requiera cifrar tam-

[27] El algoritmo RSA fue inventado en 1978 por Ron Rivest, Adi Shamir y Leonard Adleman y su nombre se debe a las primeras letras de los nombres de sus inventores.

[28] Viega, John, Messier, Matt, *Secure Programming Cookbook for C and C++*, O'Reilly, 2003.

[29] *Viega, John, McGraw, Gary, Building Secure Software, Addison Wesley,* 2002.

[30] *Op. cit.*

[31] *Viega, John, Messier, Matt, Secure Programming Cookbook for C and C++*, O'Reilly, 2003.

bién se utilice un MAC para verificar la integridad del mensaje, además de manejar adecuadamente las posibles condiciones de error.

Para la implementación de la seguridad en el voto electrónico se sugiere emplear el algoritmo de RSA debido a que es ampliamente utilizado y las operaciones con la llave privada se realizan mucho más rápido que con otros algoritmos; cuando se firma un mensaje su velocidad es similar a la de DSA, pero 10 veces más rápida en la verificación, si se implementa apropiadamente.

3. El Algoritmo RSA

El algoritmo RSA es de llave pública y permite el cifrado de datos y el manejo de formas electrónicas para la autenticación.[32] Su funcionamiento básicamente consiste en:

Seleccionar dos primos grandes, p y q, y calcular su producto $n=pq$ llamado módulo. Elegir un número, e, menor que n y primo relativo de $(p\text{-}1)$ $(q\text{-}1)$, lo cual significa que e y $(p-1)$ $(q-1)$ no tienen factores comunes a excepción del 1. Se elige otro número d tal que $(ed-1)$ es divisible por $(p-1)$ $(q-1)$. Los valores de e y d son los exponentes público y privado respectivamente. Por tanto, la llave pública sería el par (n, e) y la llave privada el par (n, d). El factor p y q debe ser destruido o guardado junto con la llave privada.

Es extremadamente difícil obtener la llave privada d a partir de la llave pública (n, e). Aun así podría factorizarse n en p y q, y por ende encontrar la llave privada d pero esto requiere de mucho procesamiento de cómputo. Por ejemplo, considerando que RSA usa números primos realmente grandes y tomando en cuenta que p y q sean de tamaño aproximado de 2^{1024}, se requiere probar si un número entre 1 y 2^{512} divide a pq, esto implica que hay que probar a todos los primos entre 1 y 2^{512}. Si se asume que una colección de computadoras pueden evaluar 100 billones de factores posibles por segundo (aproximadamente 2^{39} posibilidades cada segundo), como hay 31 536 000 (2^{25}) segundos en un año, el número

[32] R. L. Rivest, A. Shamir, and L. M. Adleman, *A method for obtaining digital signatures and public-key cryptosystems, Communications of ACM*, 1978.

posible de factores que pueden evaluarse en un año son (2^{39} evaluaciones/segundo)*(2^{25} segundos/año)= 2^{64} evaluaciones/año. Ya que hay 2^{512} posibilidades, se necesita aproximadamente $2^{(512-64=448)}$ años para determinar la mitad de las posibilidades, es decir encontrar p y q.

Por supuesto el tiempo para factorizar pq es mucho mayor que el tiempo para encontrar p y q, ya que si se seleccionan p y q como números cercanos a un millón (2^{20}), el trabajo consiste en analizar los posibles factores entre 2 y 2^{10}, esto necesita realizarse dos veces, para confirmar que p y q son primos, así el trabajo requerido es aproximadamente 2 mil comparaciones. Para factorizar pq se necesita 240, por lo que se requiere analizar entre 2 y 2^{20}, es decir, un millón de comparaciones. Lo que significa 500 veces más trabajo.

Dan Boneh[33] estableció que muchos de los ataques, aunque ninguno devastador, ilustran el peligro del uso inapropiado del RSA y que esto se debe principalmente a que la implementación del RSA no es una tarea trivial.

4. Bibliotecas criptográficas para la implementación del RSA

En las aplicaciones de *software* normalmente se utilizan bibliotecas criptográficas desarrollas por otras personas. Existen varias librerías, cada una con sus ventajas y desventajas, en la tabla 1 se presenta una comparación con algunas de las más populares.

Tabla 1 Comparación de algunas de las librerías más populares

Característica	Cryptlib	OpenSSL	Crypto++	BSAFE	Cryptix
Lenguajes y plataformas	C, multiplataforma. Bajo Windows: Delphi y otros a través de ActiveX	C, se pueden realizar operaciones a través de shell scripts	C++, muchos compiladores no pueden construirla	C y Java	Java
Algoritmos simétricos	Blowfish, TripleDES, IDEA, RC4, RC5, Rijndael	Blowfish, TripleDES, IDEA, RC4, RC5, AES	Muchos conocidos, incluyendo AES	Familia DES RC2, RC4, RC5, RC6 y AES	Muchos conocidos, incluyendo AES

[33] Boneh, Dan, "Twenty Years of Attacks Against the RSA Crypto-system", *Notices of the American Mathematics Society*, 5(2), 1999.

Característica	Cryptlib	OpenSSL	Crypto++	BSAFE	Cryptix
Algoritmos hash	SHA-1, RIPE-MD-160, MD5	SHA-1, RIPE-MD-160, MD5	Familia SHA y casi todos los conocidos	MD2, MD5 y SHA-1	MD5, SHA-1, RIPEMD-160
MACs	SHA-1, RIPE-MD-160, MD5	HMAC, para todos los algoritmos hash	HMAC, DMAC, XOR-MAC	HMAC	HMAC
Algoritmos de llave pública	RSA, El Gamal, Diffie-Hellman, DSA	RSA, Diffie-Hellman, DSA	RSA, El Gamal, Diffie-Hellman, DSA	RSA, Diffie-Hellman y DSA	RSA, El Gamal, Diffie-Hellman y DSA
Calidad y eficiencia	Robusta, bien escrita y eficiente. Muchas funciones críticas en ensamblador. Totalmente reentrante y trabaja en ambientes multi-hilos	Robusta, bien escrita y eficiente. Muchas funciones críticas en ensamblador No es la mejor opción para ambientes embebidos o cuando existen restricciones de memoria. Código reentrante	Buena implementación, baja eficiencia en UNIX	Muy eficiente y de alta calidad	Lenta
Documentación	Clara y fácil de usar	Clara y fácil de usar	Poco documentada	Muy buena	Inadecuada para programadores que nunca la han usado
Facilidad de uso	Ofrece funcionalidad de alto nivel con una interfaz de bajo nivel	La interfaz EVP (*envelope*) hacer más fácil la programación	Una vez entendida la API es fácil de usar	Promedio	Difícil por la falta de documentación
Extras	Manejo de certificación digital, passwords y llaves.	Implementación completa de SSL, aunque difícil de usar	Soporte para ECC	Depende del producto. Incluye ECC, control de memoria, manejo de llaves	Soporte para ECC
Costo	Libre para uso no comercial	Licencia libre	Libre para cualquier uso	Comercial. Entre el 6 y 3% de las ventas del producto que lo use	Libre
Disponibilidad	http://www.cs.uckland.ac.nz	http://www.openssl.org	http://www.eskimo.com	http://www.rsasecurity.com	http://www.cryptix.com

Para implementar el voto electrónico mediante el uso del algoritmo RSA se sugiere utilizar OpenSSL la cual es una de las librerías más utilizadas por su portabilidad sobre cualquier ambiente, además de que está disponible y tiene soporte para varios lenguajes de programación.

En OpenSSL existen interfaces individuales que soportan cada uno de los algoritmos, sin embargo, es preferible usar una interfaz genérica, que permita intercambiar algoritmos. Esta interfaz genérica o maestra es llamada EVP (abreviación de *envelope*). Para usar esta interfaz se incluye <*openssl/evp.h*>. Para ligar al subsistema criptográfico OpenSSL se usa la librería *libcrypto.a*, normalmente instalada en /usr/local/lib o en el *path default*.

La selección del tamaño de la llave pública se realizó de acuerdo a la tabla 2[34] con una instanciación de 2 048 bits.

Tabla 2. Longitudes recomendadas para criptografía de llaves públicas

Nivel deseado de seguridad	Algoritmos simétricos (bits)	Algoritmos de llave pública (bits)
Aceptable (probablemente segura entre 5 y 10 años)	80	1 024
Buena (posiblemente segura por siempre)	128	2 048
Alta	192	4 096
Muy alta	256	8 192

La librería OpenSSL posibilita la implementación del algoritmo RSA, y permite:

- Manipular números grandes (*BIGNUM*)
- Generar números primos
- Generar un par de llaves RSA (*RSA *RSA_generate_key (...)*)
- Convertir cadenas binarias a enteros utilizando el estándar PKCS#1, que es el más utilizado en las implementaciones de RSA
- Convertir enteros a cadenas binarias

[34] Viega, John, Messier, Matt, *Secure Programming Cookbook for C and C++*, O'Reilly, 2003.

- Encriptar y desencriptar (*int RSA_public_encrypt (...)* E *int RSA_private_decrypt (...)*)
- Firmar los datos usando la llave privada (*int RSA_sign (...)*)
- Verificar los datos (*int RSA_blinding (...)* E *int RSA_verify (...)*

5. Conclusiones

La seguridad en el voto electrónico es una parte fundamental al momento de su implementación. Como lo hemos visto el desarrollo de esquemas de seguridad es una tarea que implica mucho esfuerzo. Por ello, a la hora de implementar mecanismos de seguridad en sistemas como lo son los del voto electrónico es recomendable analizar el entorno sobre este tema y considerar la aplicación de mecanismos existentes que se encuentren certificados por organismos reconocidos como algoritmos confiables. Los desarrolladores encontraremos una serie de librerías que permiten incorporar estos esquemas de manera rápida y sencilla.

BIBLIOGRAFÍA

BONEH Dan, "Twenty Years of Attacks Against the RSA Crypto-system", *Notices of the American Mathematics Society*, 5(2), 1999.

FERGUSON, Niels, Schneier, Bruce, *Practical Cryptography*, Wiley, 2003.

VIEGA, John, McGraw, Gary, *Building Secure Software*, Addison Wesley, 2002.

VIEGA, John, Messier, Matt, *Secure Programming Cookbook for C and C++*, O'Reilly, 2003.

WELSCHENBACH Michael, *Cryptography in C and C++*, Apress, 2001.

RIVEST R. L., A. Shamir, and L. M. Adleman, *A method for obtaining digital signatures and public-key cryptosystems, Communications of ACM*, 1978.

Criptosistema para el voto electrónico con curvas elípticas utilizando campos finitos binarios con representación polinomial

Luis Manuel Callejas Sáenz
Roberto Valdivia Beutelspacher
José Eslava

Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM), campus Estado de México.

RESUMEN

Esta ponencia propone el uso de algoritmos de curvas elípticas para obtener un mecanismo criptográfico que cumpla con los requerimientos mínimos que el cómputo móvil sugiere, por lo que la implementación de estos algoritmos deberá basarse en el estándar ANSI X9.63,[35] atendiendo así el requerimiento fundamental de seguridad exigido por el Instituto Electoral del Distrito Federal (IEDF).

Para los algoritmos de curvas elípticas se pueden utilizar conjuntos de números reales, primos o binarios. Este trabajo propone curvas elípticas con conjuntos finitos de números binarios empleando la representación polinomial y se sugiere entonces que su implementación se realice por software.

El objetivo es usar menos espacio de almacenamiento, menos memoria y menos ancho de banda que otros criptosistemas, para que las implementaciones se realicen en dispositivos móviles, tarjetas inteligentes y aplicaciones con ancho de banda reducido.

[35] Acuerdo y transportación de llaves usando criptografía de curvas elípticas.

Al aplicar los algoritmos propuestos con las curvas elípticas *B-163, B-233* y *B-283*, así como la aritmética de dichas curvas en un cuerpo finito binario con representación polinomial, sobre una arquitectura de 32 bits en una plataforma pentium IV a 2.4 Ghz con 512 KB en RAM, se tiene como resultado la siguiente tabla expresada en micro-segundos (μs).

	m=163	m=233	m=283
Adición	0.10	0.12	0.13
Multiplicación	16.36	27.14	37.95

m =microsegundos

INTRODUCCIÓN

"México como otras naciones, en los últimos años comenzó a buscar una opción de democracia basada en el uso de las TI's. Esta es la denominada votación electrónica, la cual no sólo consiste en contar con la arquitectura física y lógica viable que brinde robustez y solidez, sino que además cuente con un alto nivel de seguridad lógica y física que permita al votante dar certeza de su aplicación."[36]

Con relación a la seguridad lógica, se propone el uso de algoritmos de curvas elípticas como base del criptosistema a emplear en los procesos electorales del IEDF utilizando la urna electrónica y sus sistemas de información relacionados con la administración de los votos.

Es importante recordar que el voto electrónico debe ofrecer transparencia, certeza jurídica, social y moral, a los ciudadanos y a las autoridades involucradas en dichos procesos electorales, y ahora con las limitantes del cómputo móvil, pues la urna electrónica se ha clasificado en tal categoría.

La finalidad de esta propuesta de seguridad es mantener la confidencialidad de los votos, es decir, que éstos sólo sean revelados a los individuos o instancia; garantizar la integridad del los mismos, evitando que se

[36] Proyecto UVE volumen 1, México, IEDF, 2003.

modifiquen de manera accidental o maliciosa y ofrecer la disponibilidad de los resultados en todo momento.

1. El voto electrónico

El IEDF se dio a la tarea de investigar la tecnología utilizada en el mundo, para la automatización del voto en elecciones locales y federales, la tabla 1 muestra 22 países que han diseñado proyectos de automatización del sufragio del elector.[37]

Tabla 1. Países que han diseñado proyectos de automatización del voto

País	Tipo de tecnología empleada
Argentina	Urna electrónica
Brasil	Urna electrónica
Canadá	Voto por Internet, urna electrónica
Costa Rica	Urna electrónica, voto por Internet
Chile	Voto por cajero automático
Estados Unidos de América	Urna electrónica, pantalla táctil (*Touch Screen*), contador mecánico
Panamá	Firma electrónica, voto por Internet, urna electrónica
Paraguay	Urna electrónica
Venezuela	Contador de votos (escáner)
Bélgica	Urna electrónica
Bosnia y Herzegovina	Urna electrónica
Dinamarca	Lector óptico
España (País Vasco)	Urna electrónica y contador de votos
Francia	Urna electrónica
Noruega	Lector óptico
Países Bajos	Urna electrónica, voto por Internet
Gran Bretaña	Contador de votos, voto por teléfono, voto por Internet
Filipinas	Urna electrónica
India	Urna electrónica
Japón	*Touch Screen*
Australia	Contador mecánico, pantalla táctil (*Touch Screen*), contador de votos
Sudáfrica	Firma electrónica

[37] Comisión de Organización Electoral del IEDF, *Proyecto para Desarrollar una Prueba Piloto mediante Urnas Electrónicas en un simulacro*, México, IEDF, 2003.

De estos 22 países, en 10 se ha implementado la automatización del voto. Cabe mencionar que el país que destaca es Brasil, en donde la urna electrónica se ha utilizado en tres ocasiones, y en dos de ellas con una cobertura de 100% de las casillas que se instalaron en todo su territorio durante las elecciones del 2000 y 2002. En el resto de los países los proyectos de automatización del voto aún no han tenido cobertura completa.

De acuerdo con la investigación del IEDF, los países que han automatizado el voto electrónico son:

Tabla 2. Países que han implementado mecanismos de automatización del voto

País	Tipo de tecnología
Brasil	Urna electrónica
Estados Unidos de América	Urna electrónica. pantalla táctil (*Touch Screen*), contador mecánico
Paraguay	Urna electrónica
Venezuela	Contador de votos (escáner)
Bélgica	Urna electrónica
España (País Vasco)	Urna electrónica y contador de votos
Gran Bretaña	Contador de votos, voto por teléfono, voto por Internet
Filipinas	Urna electrónica
India	Urna electrónica
Japón	Pantalla táctil (*Touch Screen*)

2. Criptosistemas

El arte de proteger la información es tan antiguo como la escritura misma. Los griegos utilizaron la palabra *criptología* (*criptos*=oculto y *logos*=tratado, ciencia) como el nombre genérico a dos disciplinas complementarias y opuestas a la vez: Criptografía y Criptoanálisis.

Los criptosistemas clásicos se ocupan solamente de la confidencialidad de la información empleando algoritmos de llave privada y métodos simétricos, donde la llave de cifrado es la misma que la de descifrado; los criptosistemas modernos garantizan la confidencialidad y autenticación utilizando llaves públicas y métodos asimétricos, donde la llave de cifra-

do es conocida públicamente y diferente a la llave de descifrado, la cual sólo es conocida por el destinatario.[38]

En un ambiente electoral, es imprescindible el uso de técnicas de cifrado y descifrado para garantizar la integridad y secrecía del voto, a su vez, las firmas digitales utilizadas en cascada permiten certificar los procesos de transmisión y recepción de la información generada en la jornada electoral, garantizando así transparencia y certidumbre jurídica y moral.

2.1 Algoritmos de llave pública

Se define un criptosistema de llave pública como una familia de funciones unidireccionales *tramposas*[39] $\{F_k\}$, *para cada llave* k de K, de modo que la trampa $t(k)$ sea fácil de obtener. Además, para cada k de K se puede describir un algoritmo eficiente que permita calcular F_k y que sea intratable la determinación de k y $t(k)$.[40]

No se ha demostrado aún la existencia de funciones unidireccionales tramposas, sin embargo, hay dos funciones candidatas a serlo. La primera es el producto de números enteros, cuya inversa es la factorización del número obtenido, y la segunda es la exponenciación discreta, y su inversa es el logaritmo discreto. Las dos funciones son fáciles de computar, mientras que no lo son sus inversas.

En la criptografía de llave secreta, a diferencia de la criptografía de llave pública, suelen presentarse tres inconvenientes:

- Distribución de llaves: dos usuarios tienen que seleccionar una llave en secreto antes de empezar a comunicarse, lo que podrán hacer personalmente o a través de un canal inseguro.
- Manejo de llaves: en una red de n usuarios, cada pareja debe tener su llave secreta particular, lo que hace un total de $n(n)$ llaves para esa red.

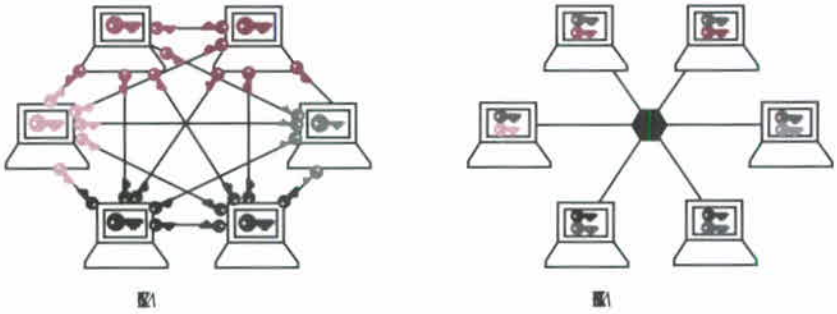
[38] W. Diffie, P. van Oorschot, M. Wiener, *Authentication and authenticated key exchanges*, 1992.

[39] Se refiere a una función que puede ser invertida fácilmente pero imposible de calcular f^1 (c)=m

[40] A.J. Menezes, P.C. van Oorschot y S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

- Sin firma digital: en los criptosistemas de llave secreta no hay posibilidad de firmar digitalmente los mensajes, por lo que el receptor del mismo no puede estar seguro de que quién le envía el mensaje es realmente quien dice ser.

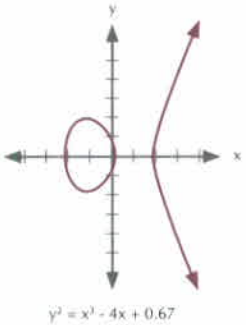
Figura 1. Criptografía de llave secreta vs. Criptografía de llave pública



2.2 Curvas elípticas

Las curvas elípticas son estructuras matemáticas determinadas por dos variables (*a, b*) y formadas por un conjunto de puntos que tienen funciones aritméticas bien definidas, usualmente la suma y la multiplicación. Una curva elíptica ofrece un conjunto de soluciones (puntos x, y) que satisfacen una determinada ecuación.

Figura 2. Curvas elípticas



Los criptosistemas de curvas elípticas utilizan menos espacio de almacenamiento, menos memoria y menos ancho de banda que otros sistemas, lo que permite implementar algoritmos criptográficos en dispositivos móviles, tarjetas inteligentes y aplicaciones con ancho de banda reducido.

Por ejemplo, el tamaño actual recomendado para las llaves de los criptosistemas públicos es de 2 048 bits, los algoritmos de curvas elípticas ofrecen el mismo nivel de seguridad con llaves de 224 bits.[41]

Otra de las ventajas de emplear curvas elípticas es que cada votante puede obtener una curva elíptica diferente, usando el mismo cuerpo finito, esto permite que todos los ciudadanos utilicen el mismo *hardware* y/o *software*. Además, la curva elíptica elegida puede cambiarse periódicamente para mayor seguridad.

Figura 3. Tamaño de las llaves para los algoritmos de curvas elípticas

NIST guidelines for public key sizes for AES

ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1 024	1 : 6	
256	3 072	1 : 12	128
384	7 680	1 : 20	192
512	15 360	1 : 30	256

Supptted by NIST to ANSI X9FT

2.3 Grupos de curvas elípticas en cuerpos finitos binarios

Los elementos de un cuerpo finito binario son secuencias de bits, por lo que las reglas de la aritmética para este tipo de cuerpos finitos se definen ya sea por una representación polinomial o por una representación normal óptima de bases. La ventaja del cuerpo finito binario sobre implementaciones de *hardware* o *software* es que la aritmética es inherente a las operaciones binarias.

[41] A.J. Menezes, P.C. van Oorschot y S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

Como ejemplo, examine el cuerpo finito binario $F_2 4$, definido por una representación polinomial con el polinomio irreducible $f(x) = x^4 + x + 1$. El elemento $g = (0010)$ es un generador para el cuerpo finito. Las potencias de *g* son:

$g^0=(0001)$ $g^1=(0010)$ $g^2=(0100)$ $g^3=(1000)$ $g^4=(0011)$ $g^5=(0110)$ $g^6=(1100)$ $g^7=(1011)$
$g^8=(0101)$ $g^9=(1010)$ $g^{10}=(0111)$ $g^{11}=(1110)$ $g^{12}=(1111)$ $g^{13}=(1101)$ $g^{14}=(1001)$ $g^{15}=(0001)$.[42]

En una aplicación criptográfica real, el parámetro *m* debe ser lo suficientemente grande (m=160) para imposibilitar la generación de las potencias de *g*, de lo contrario el criptosistema podría ser vulnerable.

Considere la curva elíptica $y^2 + xy = x^3 + g^4x^2 + 1$, donde $a=g^4$ y $b=g^0=1$. El punto (g^5,g^3) satisface la ecuación anterior:

$(g^3)^2 + g^5g^3 = (g^5)^3 + g^4g^{10} + 1$
$g^6 + g^8 = g^{15} + g^{14} + 1$
$(1100) + (0101) = (0001) + (1001) + (0001)$
$(1001) = (1001)$

Los 15 puntos que satisfacen la ecuación anterior son: $(1,g^{13})$, (g^3,g^{13}), (g^5,g^{11}), (g^6,g^{14}), (g^9,g^{13}), (g^{10},g^8), (g^{12},g^{12}), $(1,g^6)$, (g^3,g^8), (g^5,g^3), (g^6,g^8), (g^9,g^{10}), (g^{10},g), $(g^{12},0)$, (0, 1)

2.4 Aritmética de una curva elíptica en un cuerpo finito binario (F_2m)

Las curvas elípticas en un cuerpo F_2m tienen un número finito de puntos y su aritmética no sufre de errores en redondeo. Lo anterior combinado con la naturaleza binaria del cuerpo F_2m mejora el desempeño de los cálculos computacionales. Las siguientes reglas algebraicas se aplican al cuerpo F_2m.[43]

[42] Certicom, *Online Elliptic Curve Cryptography Tutorial*, 2004.
[43] *Op. cit.*

Para la suma de los puntos P y Q donde P no es $-Q$, se tiene que $P+Q=R$, $s=\frac{y_p - y_q}{x_p + x_q}$, $x_R = s^2 + s + x_p + x_q + a$, $y_R = s(x_p + x_R) + x_R + y_p$. Al igual que las curvas elípticas con números reales, $P+(-P)=O$, el punto al infinito.

Para doblar el punto P, si $x_p = 0$ entonces $2P=O$ de lo contrario $2P=R$ donde $s=\frac{x_p + y_p}{x_p}$, $x_R = s^2 + s + a$, $y_R = x_p + (s+1) \cdot x_R$. Es importante recordar que a es uno de los parámetros seleccionados para definir la curva elíptica.

2.5 Criptografía de curvas elípticas con campos finitos binarios

Los campos finitos de números primos ofrecen la mejor implementación de curvas elípticas por hardware, ya que se utilizan las compuertas lógicas embebidas en los procesadores para la aritmética de números enteros; mientras que los campos finitos binarios se aconsejan para implementaciones eficientes por software. El FIPS[44] 186-2 recomienda cinco campos finitos binarios: F_2 163, F_2 233, F_2 283, F_2 409, F_2 571; el orden de cada uno de ellos es al menos el doble de la longitud de la llave en los cifrados simétricos.

Tabla 3. Tamaños de campo indicados por NIST

Longitud de la llave simétrica	Algoritmo ejemplo	Longitud de p en F_p	Dimensión de m en F_2m
80	SKIPJACK	192	163
112	3DES	224	233
128	AES small	256	283
192	AES medium	384	409
256	AES large	521	571

Las curvas elípticas recomendadas por NIST[45] para los campos finitos F_2 163, F_2 233, F_2 283 se muestran en la tabla 4, y la notación utilizada para los elementos de F_2m es la representación polinomial cuyas operaciones aritméticas son más eficientes en software, mientras que la representación normal base ofrece mejor rendimiento en hardware; la reducción poli-

[44] Federal Information Processing Standards.

[45] National Institute of Standards and Technology.

nomial para los campos F_2 163, F_2 233, F_2 283[46] es: $f(x) = x^{163} + x^7 + x^6 + x^3 + 1$, $f(x) = x^{233} + x^{74} + 1$, $f(x) = x^{283} + x^{12} + x^7 + x^5 + 1$. Cabe recordar que una curva elíptica E sobre F_2m es especificada por los coeficientes a, b que pertenecen a F_2m; el número de puntos sobre E es nh, donde n es primo y h un co-factor; una curva aleatoria sobre F_2m se denota por B-m.

Tabla 4. Curvas elípticas recomendadas por NIST

B-163: a = 1, h = 2,						
b = 0x	00000002	0A601907	B8C953CA	1481EB10	512F7874	4A3205FD
n = 0x	00000004	00000000	00000000	000292FE	77E70C12	A4234C33
B-233: a = 1, h = 2,						
b = 0x	00000066	647EDE6C	332C7F8C	0923BB58	213B333B	20E9CE42
	81FE115F	7D8F90AD				
n = 0x	00000100	00000000	00000000	00000000	0013E974	E72F8A69
	22031D26	03CFE0D7				
B-283: a = 1, h = 2,						
b = 0x	027B680A	C8B8596D	A5A4AF8A	19A0303F	CA97FD76	45309F42
	A581485A	F6263E31	3B79A2F5			
n = 0x	03FFFFFF	FFFFFFFF	FFFFFFFF	FFFFFFFF	FFFFEF90	399660FC
	938A9016	5B04247C	EFADB307			

3. Aplicación para un criptosistema de voto electrónico

Existen tres casos que deben evitarse cuando se construyen sistemas criptográficos basados en curvas elípticas,[47] las curvas de dichos casos se consideran débiles ya que producen sistemas substancialmente vulnerables en niveles de seguridad, a saber:

- Curvas elípticas supersingulares
- Curvas elípticas modulo p, que contienen exactamente p puntos

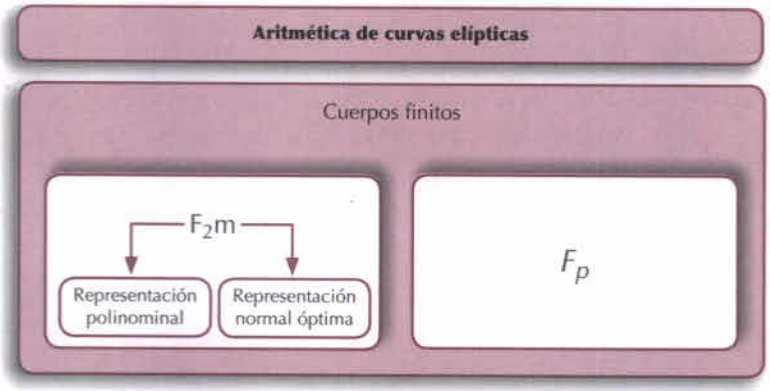
[46] Darrel Hankerson, Julio López Hernández, Alfred Menezes, *Software Implementation of Elliptic Curve Criptography Over Binary Fields*, 2002.

[47] Certicom, *The Elliptic Curve Cryptosystem for Smart Cards*, 1998.

- Curvas elípticas definidas sobre un cuerpo finito con 2^m elementos, donde m no es primo

El desarrollador o constructor que desee implementar curvas elípticas para sistemas criptográficos deberá seleccionar alguno de los dos campos finitos (números primos o binarios), curvas elípticas en un cuerpo finito F_p o curvas elípticas en un cuerpo finito F_2m. Ya se ha visto que ambos campos ofrecen la misma dificultad para el ECDLP,[48] la siguiente figura resume las opciones de implementación.

Figura 4. Opciones de implementación para curvas elípticas



A pesar de que no existen diferencias en los niveles de seguridad y estándares, en ambos cuerpos finitos sí existen diferencias de desempeño y costo para implementaciones en tarjetas inteligentes, por ejemplo, en ambientes comunes de *software*, el uso de F_2m ofrece ventajas significativas en el desempeño por la plataforma binaria utilizada y embebida en el procesador.

[48] Elliptic Curve Discrete Logarithm Problem.

Los parámetros *a* y *b*, que definen una curva elíptica, son el resultado de la función hash SHA1[49] (de un sólo sentido) y los valores de entrada a dicha función garantizan la naturaleza aleatoria de la curva, además, el uso de este método le asegura al usuario que la curva elíptica generada no forma parte de los grupos de curvas débiles descritos anteriormente.

Algoritmo 1: Generación de una curva elíptica aleatoria utilizando números binarios.

Parámetros: $s = \frac{m-1}{160}, v = m - 160 \cdot s$

Entrada: Un cuerpo finito de tamaño $q = 2^m$.

Salida: Secuencia $gen \geq 160$ bits, los elementos *a* y *b* que definen la curva elíptica *E*.

Desarrollo:

1. Seleccionar una secuencia de bits que tengan relación con la fecha, hora e identificador del voto (*gen*) de longitud $g \geq 160$ bits.
2. Calcular $H = SHA1(gen)$, donde $b_0 = v$ bits más significativos de la derecha en *H*.
3. *z* será el entero cuya expansión binaria esta dada por la secuencia *gen*.
4. De i=1 hasta *s* hacer:
   a. s_i = secuencia de *g* bits, la cual es la expansión binaria del entero $(z + i) \bmod 2^g$
   b. Calcular $b_i = SIIA1(s_i)$
5. $b = b_0 + b_1 + \ldots + b_s$.
6. Si $b = 0$ entonces ir al paso 1.
7. Seleccionar arbitrariamente el valor de $a \in F_2m$.
8. La curva elíptica generada es $E: y^2 = xy = x^3\ ax^2 + b$
9. La salida es *gen*, *a*, *b*.

[49] Secure Hash Standard Algorithm 1.

Algoritmo 2: Verificación de la curva elíptica generada de manera aleatoria por el algoritmo 1.

Entrada: Un cuerpo finito de tamaño $q = 2^m$.
Secuencia *gen* de longitud $g \geq 160$ bits.
Los elementos $a, b \in F_2m$

Salida: Aceptación o rechazo de la curva elíptica E generada con el algoritmo 1.

Desarrollo:
1. Calcular $H = SHA1(gen)$, donde $b_0 = v$ bits más significativos de la derecha en H.
2. z será el entero cuya expansión binaria esta dada por la secuencia *gen*.
3. De i=1 hasta s hacer:
   c. s_i = secuencia de g bits, la cual es la expansión binaria del entero $(z + i) \bmod 2^g$
   d. Calcular $b_i = SHA1(s_i)$
4. $b' = b_0 + b_1 + \ldots + b_s$.
5. Si $b = b'$ la curva es aceptada de lo contrario es rechazada.

4. Resultados

Al implementar los algoritmos 1 y 2 a las curvas elípticas *B-163, B-233* y *B-283*, así como la aritmética de dichas curvas en un cuerpo finito F_2m (números binarios) con representación polinomial, sobre una arquitectura de 32 bits en una plataforma Pentium IV a 2.4 Ghz con 512 Kb en RAM, se obtiene como resultado las siguientes tablas expresadas en micro-segundos (μs).

Tabla 5. Tiempos de respuesta para operaciones sobre F_2m

	m=163	m=233	m=283
Adición	0.10	0.12	0.13
Multiplicación	16.36	27.14	37.95
Karatsuba	3.92	7.04	8.01

m = microsegundos

Tabla 6. Tiempos de respuesta para multiplicación de puntos

	m=163	m=233	m=283
Curvas aleatorias			
Binarias	9 178	21 891	34 845
Window NAF con w = 4	3 440	7 971	11 997
Montgomery	3 240	7 697	11 602
Fixed-base comb con w = 4	1 683	3 966	5 919

Tabla 7. Tiempos de respuesta para multiplicación de puntos al generar firma digital

Curva	Bloqueo de memoria?	Métodos rápidos	m=163	m=233	m=283
Aleatoria	No	Fixed-base comb (w = 4)	1 683	3 966	5 919
	Sí	Montgomery	3 240	7 697	11 602
Koblitz	No	Fixed-base window TNAF (w=6)	1 176	2 243	3 330
	Sí	TNAF	1 946	4 349	6 612

5. Conclusiones

Este trabajo ha expuesto el uso, el campo de aplicación y las ventajas de los algoritmos de curvas elípticas. Es importante destacar que con el criptosistema de curvas elípticas propuesto para los procesos electorales del IEDF, cada votante obtendrá una curva diferente empleando el mismo cuerpo finito binario; dos de los parámetros para generar curvas elípticas son *a* y *h* (ver algoritmo 1), cuyos valores estarán determinado por la firma digital del presidente de casilla y por el identificador de voto (no del votante), respectivamente; de esta forma, cada voto se cifra utilizando una curva elíptica diferente, con lo cual se asegura la integridad y secrecía de los sufragios.

Como el lector puede observar, se sugiere que cada voto se cifre y se guarde cifrado una vez impreso su comprobante, mismo que contará con la impresión de la llave pública utilizada para tal fin. El objetivo de imprimir esta llave es que sirva como un mecanismo de conteo físico de los votos al final de la jornada electoral, esto es, se propone además un dispositivo contador de votos que se alimente con las copias de los comprobantes. Aclarar; este dispositivo leerá la llave pública e incrementará en 1 el contador correspondiente al partido político o coalición. Hay que

señalar que parte de la información que contiene la llave pública se refiere al partido político o coalición por la que se emitió el voto.

Las operaciones que el lector puede observar en el párrafo anterior deben ser atómicas, pues si un proceso falla deberá ser imposible contabilizar el voto. Lo anterior es de suma importancia para garantizar la transparencia de la jornada electoral al utilizar dispositivos electrónicos, asimismo para dar certeza jurídica, social y moral a los ciudadanos y partidos políticos, y con ello mejorar la calidad democrática que tanta falta hace en nuestro país.

BIBLIOGRAFÍA

PROYECTO UVE volumen 1, México, IEDF, 2003.

NSTITUTO ELECTORAL DEL DISTRITO FEDERAL, *Proyecto para Desarrollar una Prueba Piloto mediante Urnas Electrónicas en un simulacro*, México, IEDF 2003.

DIFFIE W., P. van Oorschot, M. Wiener, *Authentication and authenticated key exchanges*, 1992.

MENEZES, A.J. P.C. van Oorschot y S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

CERTICOM, *Online Elliptic Curve Cryptography Tutorial*, 2004.

HANKERSON, Darrel, Julio López Hernández, Alfred Menezes, *Software Implementation of Elliptic Curve Criptography Over Binary Fields*, 2002.

CERTICOM *The Elliptic Curve Cryptosystem for Smart Cards*, 1998.

Aplicación de *Smart Cards* en el Proceso Electoral Mexicano

Luis Manuel Callejas Saénz, Roberto Valdivia Beutelspacher, José Eslava

Instituto Tecnológico de Estudios Superiores y de Monterrey, campus Ciudad de México

RESUMEN

El presente trabajo pretende exponer el potencial de la utilización de las denominadas *Smart Cards* en el proceso electoral mexicano, de manera que permita generar tres resultados:

- La creación de un documento único de identificación nacional que pueda utilizarse en distintos procesos administrativos
- El desarrollo de un documento infalsificable y que dé certeza de identificación de votantes dentro del proceso electoral
- La reducción de costos en el proceso electoral mexicano y en muchos procedimientos administrativos en la mayoría de las dependencias públicas

De forma particular, la aplicación de *Smart Cards*, dispositivos biométricos y urnas electrónicas, permitirán que los procesos electorales sean más eficientes.

INTRODUCCIÓN

El proceso electoral mexicano en la actualidad pasa por una transformación mediante la cual se pretende migrar de los procesos del modelo de elección típico a un modelo de voto electrónico.

Para lograr lo anterior, varias entidades federativas y sus institutos electorales han comenzado a trabajar en investigar para poder desarro-

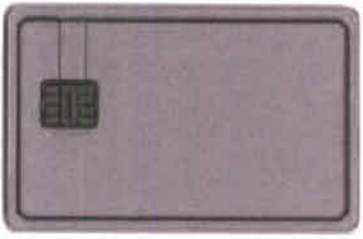
llar un modelo de votación electrónica, sin embargo, la mayoría de estas instituciones están avocadas solamente al desarrollo de tecnología, mas no de procesos que harían más eficiente la votación.

Por definición la implementación de nuevas tecnologías en una organización debe ir de la mano de un rediseño de los procesos involucrados.[50]

El proceso de producción de credenciales de elector puede ir más allá de la impresión e inserción de imágenes y texto en una tarjeta plástica. Las tarjetas inteligentes o *Smart Cards* (SC),[51] incorporan tanto cintas magnéticas como chips que pueden almacenar información electrónica más completa sobre los electores.

Una SC es una tarjeta de plástico de PVC, similar a las actuales tarjetas de crédito convencionales, que contiene un microchip de alta tecnología (véase figura 1), el cual le sirve para almacenar y procesar alguna información relacionada con el tipo de la tarjeta.[52] Al igual que las tarjetas de crédito convencionales, las SC requieren un lector apropiado para la lectura de la información contenida en el chip.

Figura 1. Estructura de una tarjeta inteligente



La SC puede tener algunas características típicas de las actuales tarjetas de banda magnética como: la impresión a color en offset, banda magnética, paneles para firmas, número de serie, realce, impresión de

[50] Ravi Kalakota y Marcia Robinson, *Del e-Commerce al e-Business*, 1a. edición, México, Addison Wesley, 2001.

[51] Mike Hendry, *Smart Card security and applications*, 2a. edición, Inglaterra, Artech House, 2001.

[52] *Op. cit.*

hologramas y personalización de chips en tarjetas de contacto y sin contacto, entre otros (véase figura 2).

Figura 2. Tarjeta inteligente personalizada

Las aplicaciones actuales de las SC son:

- Control de acceso y de presencia
- Monedero electrónico
- Identificación y autenticación
- Pagos electrónicos
- Transportes
- Identificación y seguridad en informática
- Programas de salud y sanidad
- Administración personalizada por grupos y segmentos

A diferencia del funcionamiento de la tarjeta de banda magnética en la que al efectuar cualquier transacción ésta debe ser llevada a cabo en línea, las SC permiten realizar transacciones fuera de línea, ya que mucha de la información requerida en la transacción se encuentra almacenada en el microchip y es validada localmente, garantizando con ello la seguridad de ésta.

1. Definición del problema

Este es el caso de la identificación del elector, ya que en México la identificación del votante se realiza por medio de una credencial de elector, instrumento controlado y emitido por el Instituto Federal Electoral (IFE).

Esta credencial, es además el documento oficial de identidad nacional, por lo que es de vital importancia cuidar el proceso por medio del cual se elabora. El documento es una simple credencial de plástico PVC que incluye en el frente: nombre, edad, sexo, domicilio, folio, año de registro, clave de elector, clave de estado, distrito, municipio, localidad, sección, fotografía y holograma. En su parte trasera tiene un espacio para la firma del propietario, información del IFE y una banda magnética que no contiene ninguna información, (véase figura 3).

Figura 3. Credencial de elector con fotografía

El proceso para generar en México una credencial de elector es el siguiente.

1. El solicitante de la credencial debe estar presente para proveer todos los datos requeridos, además de presentar la documentación necesaria para el trámite en cuestión.
2. La información textual se imprime en papel, después el solicitante firma el registro impreso, y coloca su huella digital.
3. El operador coloca el papel impreso con la firma o huella en un dispositivo especial y se le toma una fotografía al solicitante.
4. Por último el dispositivo imprime la credencial cubierta por una mica que incluye dispositivos de seguridad como lo son hologramas o imágenes incrustadas en el frente para evitar la alteración o falsificación de la misma.

Cabe mencionar que para realizar cualquier corrección o actualización de los datos, así como la reposición por pérdida o extravío se requiere que el elector se vuelva a presentar en las oficinas del IFE para realizar de nuevo el trámite.

Los métodos de identificación que se utilizan en el proceso electoral mexicano principalmente son visuales, es decir, en la casilla electoral los encargados se basan en la revisión visual de la fotografía, la firma y la huella digital.

Este proceso presenta varias debilidades, ya que las comparaciones de firmas y huellas digitales son actividades que requieren de gran habilidad y están sujetas al error humano, por lo que no se puede esperar que el personal de la casilla siempre tenga la capacidad técnica para realizarlas adecuadamente.

También es el caso con la fotografía, ya que la fisonomía del elector puede cambiar significativamente respecto a la foto incluida en la credencial, sobre todo si ésta no está actualizada. Pero un problema de mayor importancia es la falsificación de la credencial de elector, ya que a pesar de que las autoridades electorales de nuestro país aseguran que es infalsificable, en enero de 2004 un equipo de investigación de una televisora local comprobó que en la explanada de las oficinas centrales del Registro Civil de la Ciudad de México es posible conseguir credenciales de elector falsas.[53] Este caso, aunado a otros, denotan la debilidad de poder contar con un instrumento confiable.

2. Modelo de solución

Existen distintas etapas en el proceso electoral mexicano en las que surge la necesidad de identificar rigurosamente a una persona, una de ellas es obviamente en el momento de la votación. Con el uso de tarjetas inteligentes en las casillas electorales, se podrá reemplazar los métodos que actualmente se utiliza para verificar que una persona ya ha votado, debido a que cuando el elector inserte su credencial en la terminal lectora de tar-

[53] Documento recuperado de la fuente http://tvazteca.com.mx/noticias el 1 de febrero de 2004.

jetas inteligentes en la casilla, la tarjeta podrá al mismo tiempo identificar al elector y registrar que ya votó en el chip, evitando así que un elector pueda votar dos o más veces durante un mismo proceso electoral.

Esto se logra gracias a la gran capacidad de almacenamiento con la que cuenta una SC donde es posible almacenar el estatus de un elector en particular, por consiguiente cada vez que una tarjeta es insertada en una terminal lectora ésta verificará el estatus del elector para conferir o negar la autorización al voto.

Existen varios casos de éxito basados en el modelo presentado por este trabajo, por lo que como se puede observar, la tecnología de las SC ofrece una mayor dimensión a la palabra "seguridad", por medio de soluciones de alta tecnología fáciles de operar permitiendo la identificación y autentificación segura de los electores, ayudando con ello a eliminar fraudes que se pudieran cometer; por ejemplo: la negación de acceso a tarjetas reportadas como extraviadas o robadas.

Una de las grandes ventajas de las SC es que son un documento de identificación casi inalterable, con el cual un individuo se puede identificar o autentificar de manera más segura, además de poder realizar la autentificación fuera de línea (*off line*), ya que el software que puede contener dicha tarjeta permite hacer evaluaciones fuera de línea, de ahí su éxito como monederos inteligentes.

Entonces el proceso de autentificación de votantes podría basarse en una combinación de los siguientes dos métodos:

- Sistema biométrico de acceso, por medio del cual la huella digital serviría de llave de acceso a la votación
- Firma digital basada, en el número de credencial de elector, número de urna, número de casilla y de distrito electoral

3. Sistemas biométricos

Estos sistemas de identificación pueden ser divididos en dos grandes tipos: visuales y electrónicos. Como ya pudimos ver anteriormente, en un proceso electoral un sistema de identificación visual no se considera suficientemente confiable, por lo mismo se pueden usar los sistemas electrónicos.

Estos sistemas pueden incluir voz, huellas dactilares, imágenes de la retina del elector u otras variables biométricas digitalizadas dentro del chip de la SC para poder compararlos con las características de la persona utilizando algún tipo de lector biométrico.

4. Firma electrónica

A medida que se incrementan las transacciones gubernamentales que se pueden realizar a través de Internet, ha surgido la necesidad de un formato electrónico de prueba de identidad, también conocido como "firma electrónica", que se basa en un método de encriptamiento de información.[54]

Actualmente el encriptamiento se considera la forma más efectiva de disminuir los riesgos en el uso de tecnología que implique la codificación de información, que puede ser transmitida vía red o por dispositivos que sólo el emisor y el receptor pueden leer, como es el caso de los CD's o discos compactos.

El encriptamiento de la información tiene distintos usos en los procesos electorales ya que en éstos se envía información personal o sobre la votación a través de una red, en especial por Internet, que genera un riesgo de información sensible.

La SC está habilitada para ser programada, y de esta forma poder codificar la información contenida en ella, para poder ser leída o modificada requiere la aplicación de una llave basada en firma digital por medio de la cual se puede actualizar alguna o toda la información dentro del chip de la *Smart Card*.

La forma de encriptamiento más recomendable para este caso es la que se basa en el sistema de llave pública-llave privada. Este sistema consiste en utilizar dos llaves diferentes para cerrar y abrir los archivos y mensajes. Las dos llaves deben estar matemáticamente ligadas. Una persona puede distribuir su llave pública a otros usuarios y utilizarla para enviarles mensajes encriptados.

[54] Donal O Mahony, Michael Peirce y Tewari Hitesh, *Electronic Payment Systems for E-Commerce*, 2a. edición, Estados Unidos, Artech House, 2001.

5. Aplicación del modelo de solución

La SC sugerida para este modelo es más cara que la tarjeta que se utiliza en la actualidad, sin embargo, al ser la credencial de elector el documento oficial de identificación nacional, el costo de producción se podría solventar por medio de un acuerdo entre distintas instituciones, que considerando que esta credencial serviría como:

1. Identificación de nacionalidad
2. Credencial de elector
3. Identificador fiscal
4. Credencial del servicio medico (IMSS, ISSSTE)
5. Pasaporte
6. Licencia de conducir

De esta forma, el costo de fabricación de la credencial de elector podría ser asumido en conjunto, además de que el volumen de credencialización permitiría llegar a un costo cercano a $2.00 que comparados con el costo actual de la credencial de elector, es más alto; pero si sumamos la reducción del costo de papel, ya que al utilizar este dispositivo no se requerirían las listas del registro de electores impresas en papel, así como de tinta indeleble, puesto que la urna electrónica, en conjunto con el dispositivo biométrico y el chip de la SC,[55] validarán si el elector es quien dice ser, (validación de la huella digital en el chip vs. huella leída por el lector de huellas dactilares en tiempo real), la urna electrónica si la credencial es de un elector válido para esa casilla (la urna electrónica contiene una llave privada generada por el número de distrito y el número de casilla, que es comparado con la misma llave contenida dentro del chip con la información del votante), y por último un campo de validación de elección, que sustituye al entintado en el dedo y a la marcación en la credencial de elector (al realizarse la votación, el sistema escribe

[55] Jean-Jacques Quisquater y Bruce Schneier, *Lecture Notes in Computer Science -Smart Cards: Research and Applications*, 1a. edición, Estados Unidos, Springer Editores, 1998.

código dentro de la tarjeta que permite saber si el elector ya votó en esta elección o no).

Otra ventaja de utilizar este dispositivo, será que para actualizar los datos por cambio de domicilio, o por otra razón, no se generará una nueva credencial, sino que solamente se escribirá en el chip la nueva información.

6. Conclusiones

La aplicación de las tarjetas inteligentes o *Smart Cards* en el proceso electoral mexicano, sería el complemento idóneo, que permitiría dar por sentada la casi total automatización de dicho proceso, además que el binomio operativo urna electrónica – credencial electrónica, sería por ende un éxito.

El costo inicial de la recredencialización sería por definición alto, pero un análisis financiero del ahorro en papel, consumibles de oficina y procesos, nos arrojaría seguramente un valor positivo de ahorro muy por encima de la diferencia con el costo de fabricación actual contra el costo de fabricación de la nueva credencial.

Por otra parte, el uso de este tipo de credencial permitiría minimizar el peligro de votos fraudulentos o de delitos electorales, más específicamente, el caso de sustitución de votantes o de falsificación de credenciales.

BIBLIOGRAFÍA

KALAKOTA, Ravi y Robinson, Marcia, *Del e-Commerce al e-Business,* primera edición, México, Addison Wesley, 2001.

HENDRY, Mike, *Smart Card security and applications,* segunda edición, London, Inglaterra, Artech House, 2001.

MAHONY, Donal O., Peirce, Michael y Tewari Hitesh, *Electronic Payment Systems for E-Commerce,* segunda edición, Estados Unidos, Artech House, 2001.

QUISQUATER, Jean-Jacques y Schneier, Bruce, *Lecture Notes in Computer Science -Smart Cards: Research and Applications*, primera edición, San José, Estados Unidos, Springer Editores, 1998.

BIBLIOGRAFÍA ADICIONAL

ENGLER, Henry. y Essinger James, *The Future Banking*, primera edición, Estados Unidos, Financial Times Prentice Hall, 2001.

HASHEM, Mostafa S. y Sechrouchni Ahmed, *Protocols for Secure Electronic Commerce*, primera edición, Estados Unidos, CRC Press, 2000.

FUENTES DE INTERNET

Banamex.com. (2003), Banamex. Recuperado el 25 de noviembre de 2003 de la fuente: http://www.banamex.com

CONDUSEF, www.condusef.gob.mx/revista/proteja/art_novedades/compre_internet.htm, 21 de noviembre de 2003.

Santander Serfin.com. (2003), Uni-K. Recuperado el 25 de noviembre de 2003 de la fuente: http://www.santander-serfin.com/publishapp/schmex/html/main.htm

Shulemberger.com (2002), tarjetas inteligentes. Recuperado el 15 de octubre 2003 de la fuente: http://www.slb.com

Sema.com. (2002), Smart Cards. Recuperado el 14 de octubre 2003 de la fuente: http://www.sema.com

Telmex.com.mx (2003), Cuenta con Telmex. Recuperado el 25 de noviembre 2003 de la fuente: http://www.telmex.com.mx

IFE (2004), página del Instituto Federal Electoral. Recuperado el 1 de febrero 2004 de la fuente: http:www.ife.org.mx

Aspectos jurídicos, sociales, políticos, procedimentales, logísticos y de capacitación en el uso de la urna electrónica

La urna electrónica y los procesos en los distritos electorales locales de la Ciudad de México

Raúl Mauricio Ayala Zertuche

Profesor titular de la Universidad Nacional Autónoma de México y de la Universidad Tecnológica de México, y maestrante en Política y Gestión del Cambio Tecnológico en el Centro de Investigaciones Económicas, Administrativas y Sociales del Instituto Politécnico Nacional. En la actualidad se desempeña como consejero electoral distrital en el Distrito Electoral XIII del Instituto Electoral del Distrito Federal.

RESUMEN

Los procesos electorales o de participación ciudadana en la Ciudad de México son organizados y supervisados por los consejos distritales. En caso de cambiar el Sistema Electoral del Distrito Federal a la utilización de la urna electrónica los procedimientos que siguen los plenos de los consejos distritales cambiarán. La modificación a la legislación para integrar la votación electrónica deberá respetar el espíritu del *Código Electoral del Distrito Federal* vigente para evitar cualquier tipo de alteración en la certeza de los resultados.

ANTECEDENTES

La introducción de las votaciones electrónicas es un hecho importante en la reforma y evolución de la democracia en el Distrito Federal. No se puede pensar en desarrollo si no existe la certeza de quién o quiénes gobiernan; por ello la transparencia es fundamental para mantener la confianza de la población en general.

La evolución del sistema electoral en la Ciudad de México lleva implícitas tres situaciones diversas e importantes. En primera instancia los antecedentes históricos característicos de nuestra democracia; posterior-

mente el marco jurídico impuesto a lo largo de los años conforme a nuestras necesidades; y el avance tecnológico, que debe apegarse a la historia y a las leyes vigentes.

Historia, leyes y tecnología son la clave para dilucidar el futuro de la democracia y su sistema electoral en la capital del país, en lo que se refiere a la introducción de las votaciones electrónicas.

Hablar de la reforma electoral en México es un asunto espinoso, y generalmente los partidos políticos son muy cautelosos al momento de discutir cualquier asunto relacionado con ello. Aún así, si deseamos evolucionar y mejorar la calidad de las votaciones en el futuro debemos considerar tres conceptos fundamentales: la historia electoral, el marco jurídico y la tecnología que deberá ser construida para cumplir con la Ley.

La historia electoral del país es especial, nos marcó situaciones predominantes durante los procesos electorales y éstas, a su vez, se mantuvieron durante muchos años. Casi siempre, una pequeña clase política era la que manejaba los hilos políticos o gubernamentales, mientras que el resto de la población estaba completamente al margen de la elección de representación popular.

Al inicio del México independiente la elección era indirecta, sólo podían votar las personas con alto nivel económico, intelectual y con capacidad para injerir en los asuntos de gobierno. Eran personas cuyo soporte económico les permitía educar con calidad a sus vástagos, el resto de la población no tenían los recursos para hacerlo.

Así, este pequeño grupo político, de manera indirecta, elegía a los gobernantes; la población en general no participaba en los procesos. De este modo se redactó la constitución de 1824, elaborada por la alta clase económica, militar y de Gobierno de la época.[56]

La dictadura de Porfirio Díaz también realizó cambios en la estructura electoral de manera que los diputados sirvieran a sus intereses. No había espacio para opiniones distintas a las del dictador, y al final de su man-

[56] Raúl Armando Quintero Martínez, "La Reforma Política del Distrito Federal", *Memoria del Foro sobre la Reforma Política del Distrito Federal*, México, Instituto Electoral del Distrito Federal, 2001, p. 39.

dato, cuando las hubo, sucedieron los primeros asesinatos de diputados muertos por sus opiniones.

La Revolución de 1910 estalló debido a que un gran sector de la población no creyó en la legítima y enésima elección de Díaz como presidente de la República. Al desconocer el procedimiento electoral se dio lugar al levantamiento armado de grupos en diversos frentes del país, ya que consideraban a aquellas elecciones fraudulentas.

La calma política llegó cuando se conformó el Partido Nacional Revolucionario (PNR) organizado por Plutarco Elías Calles, quien reunió a las fuerzas políticas dispersas por todo el país. Así surgieron los partidos políticos con un corte moderno y ello trajo consigo nuevos procedimientos para realizar las elecciones, aunque estos fueron para beneficiar al partido oficial y de gobierno.

El primer partido de oposición real fue Acción Nacional fundado en 1939, pero fue totalmente opacado por las elecciones amañadas de la época, ya que éstas sólo sirvieron para confirmar los deseos del presidente en turno. El PNR cambió de nombre a Partido de la Revolución Mexicana (PRM) y posteriormente, en 1941, se convirtió en el actual Partido Revolucionario Institucional (PRI).

Sin embargo, no había posibilidad alguna de representación por parte de la oposición, no había diputados, mucho menos senadores, todo lo acaparaba el partido en el gobierno. Fue hasta 1977 cuando se aprobó la *Ley Federal de Organizaciones Políticas y Procesos Electorales,* misma que permitía a los pequeños partidos políticos acceder, por medio de la representación proporcional, a algunas curules en la Cámara de Diputados. De hecho, por vez primera varios diputados, no pertenecientes al PRI, tomaron protesta como tales; en la actualidad se considera esto como el punto de arranque para la competitividad electoral en el país.[57]

Pero en 1988 sobrevendría lo peor en la historia electoral de México: un grupo de militantes priístas participaron en las elecciones, pero abanderando a otros partidos políticos y no al oficial. Cuauhtémoc Cárdenas

[57] Alejandro Moreno, *El votante mexicano, democracia, actitudes políticas y conducta electoral,* México, Fondo de Cultura Económica, 2003, p.11.

Solórzano se convirtió en candidato por el Frente Democrático Nacional (FDN), mientras que Carlos Salinas de Gortari lo hacía por el PRI. El resultado de aquellos comicios está catalogado por la voz popular como un fraude electoral de gran magnitud que causó *"un cúmulo de insatisfacciones de la población y exigencias de cambio"*.[58]

Basta recordar la frase dicha por Manuel Barlett Díaz, entonces secretario de Gobernación, en la madrugada del 7 de julio de 1988: "Se cayó el sistema"; o, cuando un aspirante a diputado (Salgado Macedonio) vació costales con boletas quemadas cruzadas como votos para el FDN y tantas otras atrocidades convalidadas en 1991 por la legislatura de la Cámara de Diputados que aprobó la quema de toda la documentación electoral referente a ese año; con esto nos damos cuenta de lo débil de las instituciones electorales del país, en particular de la Comisión Federal Electoral.

Aquello fue el tope que la ciudadanía podía aguantar, los gobernantes no tenían la legitimidad para gobernar y cuando lo hacían sólo representaban sus intereses particulares y nunca el bienestar común. Las reformas a las leyes comenzaron, en 1991 se conformó el Instituto Federal Electoral (IFE) aunque controlado todavía por el Poder Ejecutivo Federal en la persona del secretario de Gobernación. Pero la Constitución ya había sido modificada y ello significaba un avance.

Se creó el *Código Federal de Instituciones y Procedimientos Electorales* (COFIPE) donde se comienza a establecer reglas claras para evitar el fraude electoral:

- En primera instancia se instaura la credencial de elector con candados de seguridad que la hacen casi infalsificable, además de otro requisito necesario para votar que es estar inscrito en la lista nominal, es decir, las dos cosas juntas, si una falta no se puede emitir el voto.
- La impresión de las boletas electorales se debe realizar de acuerdo a ciertos requisitos, tales como papel seguridad especialmente hecho

[58] Enrique Montero Ponce, "Política y medios de comunicación", *La democracia en Marcha*, Dirección General de Radio, Televisión y Cinematografía, Colección Intermedios, México, 1992, p. 98.

para la elección, y un folio para cada papeleta, ya que la casilla no puede tener más de las que por ley tiene asignadas.
- En cuanto a las urnas, éstas deben ser de material transparente para poder observar el interior.
- Asimismo, se estableció que los funcionarios de casilla se insaculan en un proceso supervisado por todos los partidos políticos y éstos deben cumplir requisitos como: no ser dirigentes de un partido político o tener un alto cargo en cualquiera de los gobiernos.

Los anteriores candados legislativos quedaron integrados en el COFIPE, porque la historia nos enseñó que justamente en los procedimientos comunes era donde se fraguaba el fraude electoral.

En 1996 se da una nueva reforma electoral y ahí se vuelve a instaurar el Sistema Electoral del Distrito Federal. Se estipula que en 1997 se elegirá a un jefe de Gobierno, lo que no sucedía desde 1928 cuando un decreto del presidente Álvaro Obregón dejó en la personalidad presidencial el poder nombrar un regente del Departamento del Distrito Federal.[59]

Aunque fue el IFE quien organizó las elecciones de 1997, se creó una nueva estructura para conformar el Instituto Electoral del Distrito Federal (IEDF) para constituirse como organismo autónomo dentro de los límites de la Ciudad de México y con ello toma forma el Sistema Electoral del Distrito Federal.

El *Código Electoral del Distrito Federal* (CEDF) sustenta jurídicamente al IEDF y ahí se encuentran las bases del sistema de elecciones en la capital del país. Existen las figuras de diputados locales para la Asamblea Legislativa del Distrito Federal y la de delegado político que gobierna los destinos de las delegaciones en que está dividida la Ciudad de México. También está facultado para recibir la votación referente a los plebiscitos y algún referéndum que por ley sean convocados.

[59] Ernesto Herrera Tovar, "El sinuoso proceso de la reforma política en el Distrito Federal", *Memoria del Foro sobre la Reforma Política del Distrito Federal*, México, Instituto Electoral del Distrito Federal, 2001, p. 28.

Aquí es cuando se da ya una innovación, se incluyen los procesos de participación ciudadana como el plebiscito y el referéndum, situación que no existe a nivel federal. Y desde el inicio se ha mantenido una actitud innovadora al llevar a cabo eventos que faciliten la elección, como es mantener sólo tres personas en la mesa directiva de casilla en comparación de las cuatro para una casilla federal.

En ese tono de innovación es necesario dar mayor claridad a las elecciones y cumplir los principios rectores de certeza, legalidad, independencia, imparcialidad, objetividad y equidad con la instauración de un sistema electrónico de votación donde la manipulación de documentos por la mano humana se reduzca al mínimo.

La introducción de una urna electrónica en toda elección implicaría aplicar los conceptos de imparcialidad, objetividad y equidad en su máxima expresión. Imparcialidad, porque será una máquina quién procese los votos ciudadanos, de este modo se logra la objetividad, los resultados son la suma aritmética realizada por la propia urna. Y, finalmente, equidad porque sin la participación humana las condiciones son iguales para todos.

Por tanto, los cambios que existan en el sistema electoral del Distrito Federal deben apegarse a la legislación actual, ya que ella es la expresión directa de la evolución electoral dentro de la historia de México. De ninguna manera deberá ser traicionado el espíritu de la misma y, aun cuando el sistema sea modificado, deberá haber candados de seguridad similares a los que marca el CEDF vigente.

1. Propuesta

La propuesta es referente al procedimiento que deberá seguir el consejo distrital para realizar sus funciones principales al organizar los procesos electorales y de participación ciudadana. Según el CEDF "en cada distrito electoral funcionarán durante el proceso electoral los Consejos Distritales, que se integrarán de acuerdo a lo siguiente: un consejero presidente y seis consejeros electorales con derecho a voz y voto".[60]

[60] *Código Electoral del Distrito Federal*, Gaceta Oficial del Distrito Federal, 30 de diciembre de 2003, p. 40.

Es un hecho legal que a nivel distrital se tiene la responsabilidad de organizar y supervisar el proceso electoral. Con la integración y participación de los ciudadanos en las mesas directivas de casilla, y la labor de los miembros del servicio profesional electoral se logra la mezcla perfecta que coadyuva a dar certeza en la organización de las elecciones y de los procesos de participación ciudadana.

El pleno del consejo electoral debe llevar a cabo sesiones para aprobar las diferentes etapas del proceso electoral. En caso de introducir un sistema electrónico de votación los procedimientos para cumplir sus atribuciones mencionadas en el Código deberán modificarse.

Para hacer el planteamiento de un nuevo procedimiento que permita utilizar la urna electrónica dentro del consejo distrital al momento de organizar un proceso electoral o de participación ciudadana es obligatorio iniciar con la configuración de dicha urna. La creación de ella la ha comenzado el IEDF, por consiguiente, mientras no exista un prototipo público será necesario (para efectos de esta propuesta) partir de esta configuración inicial.

La urna electrónica deberá cumplir al menos con lo siguiente para que tenga una validez legal:

- Un sistema operativo propietario que contenga únicamente las instrucciones básicas y que no permitirá ejecutar comandos por medio de un dispositivo externo.
- Un panel de dispositivos con capacidad de ser sellado para posteriormente poderlo abrir.
- Dispositivos de lectura y grabación de datos:
  - Dos tarjetas de memoria extraíbles (*flash, stick, secure data*, etcétera.)
  - Un chip de seguridad empotrado en la tarjeta madre de la urna y sólo podrá ser leído por medio de un software especial de la Computadora Central Distrital (CCD).
- Capacidad de leer la banda magnética de la credencial de elector.
- Dar acceso al voto sólo a quién aparezca en el listado nominal de la sección correspondiente.

- La base de datos de la urna electrónica debe hacer referencia a la lista nominal de electores de la sección y al listado de candidatos y partidos políticos para todas las elecciones.
- La pantalla de la urna deberá ser a colores con un tamaño mínimo de siete pulgadas.
- Contener en su interior una impresora para poder presentar en papel seguridad las diversas actas a entregar a los representantes de los partidos políticos.
- El tamaño y peso total de la urna deberá ser considerado para dar facilidad en su manejo y conexión, así como independencia a la corriente de electricidad.
- Deberá haber una CCD donde se concentren los datos para poder hacer el cómputo de votos en el Distrito electoral como marca la ley.
- Los conectores entre los puertos de la urna electrónica y la CCD deberán ser propietarios del IEDF y de ninguna manera comerciales.
- La CCD deberá tener instaladas algunas tarjetas PCI para poder interconectarse con las diferentes urnas electrónicas.
- El *software* de la CCD también tendrá que contar con sus lineamientos propios de programación con capacidad para ser auditado y de preferencia con un sistema operativo no comercial.
- La CCD no podrá tener instalado ningún otro tipo de software que no sea el adecuado para sus funciones (esto puede ser motivo de delito electoral).
- La CCD deberá tener la capacidad de conectarse en red para combinarse con el Programa de Resultados Electorales Preliminares (PREP).
- La conexión a la red que interconecte el nuevo sistema electoral del Distrito Federal deberá ser 100% segura.
- El encriptamiento de los datos electorales que viaje por cualquier medio o protocolo de comunicación deberá ser de altísimos niveles de seguridad.
- La CCD deberá tener la capacidad de auditarse en cualquier momento, desde los procedimientos, usuarios, modificaciones, instalaciones de programas de cómputo, así como en los parámetros de programación.

La necesidad de contar con una configuración inicial tentativa es porque se replantearán todos los procedimientos de los procesos electorales o de participación ciudadana en los consejos distritales, es decir, que todas las acciones que se hagan se basarán en los contenidos de la urna electrónica y en los dispositivos para almacenarlos de manera confiable.

La organización de los procesos electorales a nivel distrital comienza con cuatro eventos: la insaculación de los funcionarios de mesa directiva de casilla (MDC), la selección de los domicilios donde éstas se instalarán, la selección de las personas que fungirán como los responsables de capacitar a los futuros funcionarios; por último, el registro de candidatos, aunque esto muy pocas veces sucede en el ámbito distrital, usualmente se realiza ante el Consejo General del IEDF.

La propuesta sugiere que los eventos de insaculación de funcionarios y la selección de los domicilios de las MDC se mantengan igual, sin modificación alguna. Sin embargo, los requisitos de los responsables de la capacitación deberán ser personas con conocimientos de informática y para ello se solicitaría el apoyo de estudiantes de ciertas licenciaturas con el objetivo de ofrecerles que cumplan su servicio social en el IEDF.

Es de hacer notar que cada distrito deberá tener una urna electrónica por sección electoral que dé un total parcial, además de sumar 5% de excedente sobre el anterior número para cualquier emergencia, las cuales servirían para realizar la capacitación.

Por ejemplo: en el Distrito Local XIII existen 175 secciones electorales,[61] por lo normal se instalan las tres MDC especiales que son permitidas por el CEDF; en total serían 178 urnas electrónicas más nueve urnas de excedente (5%) para capacitación o emergencia durante la jornada electoral, lo que da un total de 187.

A partir de este momento los procedimientos cambiarían de manera radical para adaptarlos a la urna electrónica, sin embargo, se enfatiza que se debe mantener el espíritu de la legislación vigente. El consejo distrital supervisa la recepción del material y la documentación electoral, tal y como

[61] Instituto Electoral del Distrito Federal, *Configuración de los distritos electorales, por delegación política*, México, IEDF, 2002.

dice se hace referencia en el Código: "las boletas y actas de casilla deberán obrar en poder del Consejo Distrital diez días antes de la elección".[62] En este sentido si habría un cambio radical, ya que hay que verificar que cada una de las urnas electrónicas en poder del consejo distrital esté vacía en su dispositivo de memoria.

En el caso del Distrito Local XIII sería hacerlo 178 veces, más las adicionales (nueve) pero en el momento cuando se cierren las etapas de capacitación. Para ello es necesario un tiempo mayor (30 días) previo a la elección para ejecutar la carga de las máquinas. El procedimiento de carga de las urnas electrónicas ante el consejo distrital deberá ser el siguiente:

- La carga implica: verificar que no haya datos dentro de las dos tarjetas de memoria extraíble y en el chip interno de seguridad emitiéndose el acta respectiva.
- Introducir a la memoria de la urna electrónica la base de datos que incluye el libro electrónico de la lista nominal correspondiente a la sección, así como la lista de candidatos y partidos políticos para todas y cada una de las elecciones.
- Se verifica y se audita la base de datos y el funcionamiento de la urna, se acepta y se procede a sellarla con dos candados diferentes entre sí, es importantísimo para la certeza de la elección que los dispositivos de memoria y espacios de conexión (puertos) estén totalmente resguardados, a excepción de la ranura de impresión.

A lo anterior se le podría llamar como la primera auditoría de la urna electrónica, sin embargo, es básico iniciar simultáneamente el proceso de capacitación de los posibles funcionarios ya insaculados. La idea es realizar dos etapas de capacitación, la primera de manera general con un sistema que permita evaluar la asimilación de conocimientos. Los resul-

[62] *Código Electoral del Distrito Federal*, Gaceta Oficial del Distrito Federal, 30 de diciembre del 2003, Artículo 176

tados servirían para seleccionar a los mejores, aquí comenzaría la segunda etapa donde se haría una capacitación más particular, igualmente evaluada, y a partir de los resultados se generarían los listados de funcionarios de MDC.

La propuesta incluye la reducción de funcionarios para participar en la jornada electoral en cada sección. En la actualidad son tres personas, la idea es que sean dos. También será obligatorio crear la figura de asistente técnico electoral, podría ser diferente al asistente electoral actual o añadirle requisitos de conocimientos en el área de la informática. Así los funcionarios de la MDC pueden apoyarse en alguien con capacidad técnica en caso de falla.

La entrega de la urna electrónica al presidente de casilla se debe de hacer no sólo de manera física sino se deberá de corroborar los conocimientos del funcionario, en ese momento se realiza una segunda auditoría a la urna electrónica con dos objetivos fundamentales: verificar que la urna se encuentre sin dato alguno en los dispositivos de memoria cuyo acceso está sellado al imprimir un acta en ceros y que el libro electrónico de la lista nominal de electores corresponda a la sección electoral donde se encuentra asignado el funcionario. Este proceso deberá ser como esta escrito en el Código, se "entregarán a cada Presidente de Mesa Directiva de Casilla dentro de los cinco días previos al anterior de la elección".[63] Y el acta resultante deberá ser entregada al consejo distrital.

La jornada electoral tendrá que iniciar con el arranque de la urna electrónica ante los representantes de los partidos políticos. Se emitirá un acta para verificar que no hay datos en el interior de la máquina y que los dos sellos se encuentren debidamente cerrados, puede ser considerada como una tercera auditoría a la urna electrónica consignada en el formato de apertura de casilla y firmada por los representantes de los partidos políticos. Así se realiza la apertura de la casilla, donde deberá ser respetado al pie de la letra la fracción II del Artículo 191 del CEDF vigente para que el ciudadano pueda emitir su voto:

[63] *Op cit.* Artículo 179.

"Los electores deberán mostrar su credencial para votar con fotografía. Los Presidentes de casilla permitirán emitir su voto a aquellos ciudadanos cuya credencial para votar con fotografía contenga errores de seccionamiento, siempre que aparezcan en la lista nominal de electores con fotografía correspondiente a su domicilio, comprobarán su residencia en la sección correspondiente por el medio que estimen más efectivo;"

En este sentido no deberá haber cambio alguno, de hecho la presencia de los funcionarios de casilla será para ello. Deberán verificar que la fotografía de la credencial para votar corresponde al elector que la porta y que hará uso de la urna electrónica; posteriormente la máquina verificará que los datos correspondientes a la credencial se encuentran en el libro electrónico de la lista nominal; si lo anterior es correcto el ciudadano podrá emitir su voto en caso contrario la urna no lo permitirá. Al salir uno de los funcionarios le entregará su credencial y se le aplicará tinta indeleble al pulgar del elector o votante.

La acción de permitir la entrada a la urna al elector después de verificar su identidad con la credencial para votar con fotografía, y que después la máquina le permita votar si aparece en la lista nominal no puede ni debe tener cambios, no importa si el sistema electoral se vuelve electrónico.

El cierre de la jornada debe dejar constancia por medio de un procedimiento para clausurar la mesa directiva de casilla:

- Los representantes de los partidos políticos verificarán la ejecución del comando de cierre de la urna electrónica.
- Se imprimirá en papel seguridad las actas de los resultados de la votación.
- Se firmará en el único formato en papel donde se verifica, se acepta la apertura y el cierre de la jornada electoral.
- La urna electrónica siempre bajo resguardo del funcionario será entregada en las instalaciones del distrito correspondiente.

En caso de emergencia la urna electrónica podrá ser sustituida de inmediato para reanudar la elección, se deberá cumplir con el mandato del código: "iniciada la votación no podrá suspenderse salvo caso fortuito o

causa de fuerza mayor",[64] sin embargo, la urna pasmada o bloqueada deberá ser entregada de inmediato al consejo distrital.

Cuando llegue la primera urna electrónica a la sede del consejo distrital dará inicio el cómputo distrital, todo deberá realizarse con base en el siguiente método:

- La urna electrónica es presentada ante el pleno del consejo distrital.
- La urna se abre al romper los sellos para poder tener acceso a los puertos de conexión y a las tarjetas de memoria extraíbles.
- Se conecta la urna a la CCD.
- Se leen los resultados de la tarjeta número uno y se proyectan los resultados en una pantalla a la vista del Pleno.
- Se cantan los resultados.
- En caso de problemas con la lectura de la tarjeta uno, se sigue el mismo procedimiento con la tarjeta de memoria extraíble de respaldo; sí los problemas continúan se ingresará el código de seguridad (*password*) para poder acceder al chip interno de seguridad y así leer los resultados almacenados en su memoria.
- Sí por causas de fuerza mayor existen dos o más urnas electrónicas por sección se procederá a realizar la sumatoria de los resultados de cada una.

Una vez cantados los resultados se imprimen las actas necesarias para integrar el expediente electoral y son firmadas por los integrantes del consejo distrital. Este procedimiento deberá seguirse casilla por casilla y desde la CCD, aunque se busca una elección electrónica, por el momento se debe dejar constancia impresa de los resultados con firmas originales para darle autenticidad.

Así será posible emitir resultados horas después de terminada la elección, sin necesidad de mantener el PREP. El mismo sistema permitirá ir viendo los resultados según ingresen y cantados en cada una de las CCD,

[64] *Ibid.* Artículo 190, párrafo segundo.

ya que ésta se conectará a una red entre los 40 distritos electorales y desde un Centro de Cómputo Central (CCC) se reemitirán los resultados, tal y como vayan llegando al servidor.

La introducción de la urna electrónica en los procesos electorales o de participación ciudadana implica cambios de fondo en la legislación actual pero deberá respetarse el espíritu de la legislación vigente. La supervisión ciudadana será parte del cumplimiento de los principios de certeza e imparcialidad y el procedimiento para manejar la urna será para darle objetividad a una votación electrónica que tiene que ser instaurada en el sistema electoral del Distrito Federal.

2. Conclusiones

Cambiar el actual sistema electoral implica como primer paso modificar la estructura legal, sin ello no es posible. Posteriormente, a partir de los cambios a la ley, se deberá realizar la configuración de la urna electrónica, entonces, será obligatorio crear una Norma Oficial Mexicana (NOM) que permita auditar y probar todos los sistemas utilizados para procesar los votos. La NOM es a nivel nacional, por lo tanto si se de no sólo sería para los habitantes de la capital.

Una urna electrónica es un dispositivo que permite concentrar los votos durante la jornada electoral en el marco de los requerimientos que establece el CEDF, salvaguardando siempre la confidencialidad y el secreto del voto. Además debe cumplir los requisitos de impresión de las diversas actas necesarias para abrir y cerrar el proceso en la mesa directiva de casilla, mismas que, por la vigencia del Código, deben tener acceso los partidos políticos acreditados en la sección electoral.

La urna electrónica no sólo tendrá que ser confiable para guardar los resultados, sino que no deberá ser complicada su utilización. La población tiene diversos niveles de interrelación con equipos electrónicos, algunos ni siquiera conocen un aparato electrónico diferente a la radio o la televisión. Aún así no debe haber dificultad para su uso, toda persona deberá poder usarla para emitir su voto sin complicación alguna.

Sin embargo, lo más importante se encuentra en el procedimiento a seguir por las autoridades electorales para validar la votación emitida por

medio de la urna electrónica. La metodología empleada en la actualidad es un proceso largo que puede durar entre uno y tres días, por ello es necesario reducir tiempos, al cambiar a un proceso de votación electrónica.

Para ello los procesos realizados en el seno de los consejos distritales, integrados por ciudadanos, deberán dar certeza a los resultados emanados de un proceso electoral o de participación ciudadana manejado de manera electrónica. Todo lo realizado en el consejo distrital se proyecta en los resultados de la elección y es ahí donde se crea la independencia, la imparcialidad, la equidad y la objetividad, no importa si se llevó a cabo de forma tradicional o electrónica, el Pleno del Consejo debe ser el fiel de la balanza.

Otro beneficio es la economía en dos sentidos: por un lado los costos de una elección son demasiado cuantiosos como para sostenerlos en un país con tantas carencias como México y por otro lado la disminución del desperdicio de papel, se elabora una boleta por ciudadano inscrito en el padrón, pero si el ciudadano no vota esas boletas deben destruirse; pensando en un margen de abstención de 50%, se desperdicia la mitad de las boletas emitidas. Estamos obligados a reducir los costos de las boletas impresas para hacer menos onerosas las elecciones en México y volverlas sustentables económica y ecológicamente.

El futuro del Sistema Electoral del Distrito Federal se debe basar fundamentalmente en el CEDF. No se puede pensar en una proposición de cambio tecnológico sin las modificaciones al marco jurídico. Una vez que los partidos políticos se pongan de acuerdo en una reforma tecnológica electoral se podrá pensar en la configuración de los diversos equipos.

La tecnología electoral deberá tomar en cuenta la historia electoral del país y continuar con todos los candados necesarios para evitar volver a un pasado electoral que nadie quiere recordar. Hagamos honor a todos los mexicanos que sólo pedían unas elecciones claras y transparentes, seamos congruentes y respetemos su lucha histórica. La votación electrónica deberá ser igual o más certera, independiente y transparente como lo es en la actualidad.

Cambiar nuestro sistema electoral es posible, nos encontramos en el momento tecnológico para hacerlo. Los equipos, dispositivos y sistemas

de transmisión de datos han evolucionado a pasos agigantados, será necesario basarse en ellos y utilizar la tecnología actual para establecer un sistema de votación electrónica en la Ciudad de México.

BIBLIOGRAFÍA

QUINTERO Martínez, Raúl Armando, "La Reforma Política del Distrito Federal", *Memoria del Foro sobre la Reforma Política del Distrito Federal*, México, Instituto Electoral del Distrito Federal, 2001.

MORENO, Alejandro, *El votante mexicano, democracia, actitudes políticas y conducta electoral*, México, Fondo de Cultura Económica, 2003.

Código Electoral del Distrito Federal, Gaceta Oficial del Distrito Federal, México, 30 de diciembre de 2003.

INSTITUTO ELECTORAL DEL DISTRITO FEDERAL, *Configuración de los distritos electorales, por delegación política*, México, IEDF, 2002.

MONTERO Ponce, Enrique, *Política y medios de comunicación. La democracia en Marcha*, Dirección General de Radio, Televisión y Cinematografía, Colección Intermedios, México, 1992.

La urna electrónica, nuevas reformas jurídicas

Lic. Mariana Montiel Martínez
Facultad de Estudios Superiores, campus Aragón
Universidad Nacional Autónoma de México

Licenciada en Derecho. El tema de su tesis fue: "La urna electrónica como solución al abstencionismo en las votaciones populares". Ha desempeñado distintos cargos del sector público y ha sido visitadora domiciliaria en el Distrito 23 del Instituto Federal Electoral y asistente electoral en el Distrito Electoral XXXI del Instituto Electoral del Distrito Federal en las elecciones locales 2003.

RESUMEN

La tecnología de vanguardia en el ámbito electoral hace posible que exista hoy un sistema que permite agilizar la organización de un proceso electoral y el desarrollo del procedimiento de la emisión del voto, este sistema tecnológico es conocido como urna electrónica y tiene como objetivo principal el dar confianza al ciudadano para que éste emita su voto en la jornada electoral con seguridad, certeza y legalidad. Por lo anterior, se deben analizar los puntos de vista político, sociológico, tecnológico y jurídico, para determinar la incorporación de dicho sistema en los procesos de elección del Distrito Federal.

INTRODUCCIÓN

La materia electoral está reglamentada por el Derecho Electoral que es el conjunto de normas jurídicas que regulan un proceso de elección popular donde los ciudadanos expresan sus decisiones a través del sufragio, con medios que permiten su emisión y de forma democrática.

En la Institución de la Democracia, el ciudadano es el principal actor por que decide quién lo gobierna y en qué forma; este acto lo realiza mediante el voto en elecciones populares que están a cargo de una ins-

titución que debe garantizar que su derecho a votar no se ignore. Así, en cada proceso electoral se presenta la necesidad de modernizar los sistemas que posibiliten agilizar la emisión del voto, lo que implica considerar reformas a la legislación electoral.

1. Reformas al *Código Electoral del Distrito Federal*

El voto es un derecho que la Ley Suprema otorga a quienes tenemos la calidad de ciudadano, y por medio del cual elegimos a los representantes políticos que nos han de gobernar.

Cuando un ciudadano mexicano cumple con los requisitos que establece el Artículo 34 de la *Constitución Política de los Estados Unidos Mexicanos* tiene derechos políticos, y uno de ellos es el de votar, mismo que incluye una obligación. Estos preceptos se fundan en los Artículos 35 y 36 de la Constitución.

Para los ciudadanos del Distrito Federal este derecho se encuentra plasmado en el *Estatuto de Gobierno del Distrito Federal*, en el Artículo 20, fracción I, y 23, fracción I; y en el *Código Electoral del Distrito Federal* (CEDF), en el Artículo 4, inciso *a*), y 5, inciso *a*). Además, para ejercer el derecho al voto los ciudadanos deben estar inscritos en el Registro Federal de Electores, contar con la credencial para votar con fotografía y estar en pleno ejercicio de sus derechos políticos.

Las reformas electorales no están enfocadas a modificar estos preceptos, toda vez que el derecho al voto será el mismo en caso de adoptarse el modelo de la urna electrónica para la emisión del voto ciudadano en los procesos electorales y de participación ciudadana, sin embargo, sí se deben plantear reformas al CEDF en los siguientes aspectos:

1.1. Libro quinto, De los Procesos Electorales y de Participación Ciudadana, Título Quinto Capítulo III

Los términos en cuanto a la aprobación del material y de la documentación electoral para la emisión del voto cambiarían por el término de la aprobación del uso y manejo de la urna electrónica para la emisión del voto ciudadano, la cual sería autorizada por el Consejo General del Instituto Electoral del Distrito Federal. Así, la lista nominal de electores

con fotografía, las boletas electorales y las actas de la jornada electoral estarían en una base de datos a través de programas informativos contenidos en la urna electrónica, dichos programas tendrían las medidas de seguridad para brindar certeza, legalidad y transparencia en el proceso electoral.

1.2. Libro Sexto, De la Jornada Electoral, Cómputos y Nulidades, Título Primero Capítulo I Disposiciones Preliminares

Se tomarían las medidas adecuadas para la recepción y distribución de las urnas electrónicas, con el personal que así disponga el Consejo General del IEDF y los consejos distritales.

En el proceso de instalación y apertura de casilla, una vez reunidos los funcionarios de casilla y los representantes de los partidos políticos, revisarían que las instalaciones sean las adecuadas para la recepción del voto. A la hora establecida por la ley el presidente de casilla procederá a imprimir el acta de la jornada electoral para constatar que la urna está vacía, la que será firmada por los funcionarios de casilla y los representantes de los partidos políticos o coaliciones. Posteriormente se procederá a recibir la votación de los ciudadanos de acuerdo a los siguientes criterios:

- Los electores votarán conforme lleguen. Una vez que asista el elector a la mesa directiva de casilla, el presidente le solicitará su credencial de elector con fotografía para confirmar que sea el mismo de la foto.
- Acto seguido el secretario introducirá la clave de elector para darle acceso.
- El elector se dirigirá a la urna electrónica y procederá a votar de acuerdo a su preferencia política, ya sea confirmando, corrigiendo o votando en blanco.
- Una vez que el elector haya votado, se dirigirá nuevamente con el pres dente de casilla a recoger su credencial para votar con fotografía.
- El Consejo General del IEDF, incluirá las claves de elector de los representantes de los partidos políticos en las mesas directivas de casilla donde se encuentren acreditados para que ejerzan su derecho al voto.

- Cuando todos los electores hayan votado, el presidente de casilla, conforme a lo establecido en la ley procederá al cierre de la misma. Acto seguido, el secretario acentará en el acta de jornada electoral, la hora y el total de votos que recibió cada candidato, partido político o coalición de la elección de que se trate, así como los votos en blanco emitidos, esta acta será firmada por los funcionarios de casilla y por los representantes de los partidos políticos. Y el secretario extraerá el disquete con los resultados totales de la jornada electoral.
- En el acta de la jornada electoral sólo estarán impresos los votos válidos para el candidato, partido político o coalición de la elección de que se trate y los votos en blanco que hayan emitido los electores.
- Concluidas las atribuciones que el Código señala para los funcionarios de la mesa directiva de casilla, el secretario levantará constancia de la hora de clausura de la casilla y el nombre de los funcionarios y representantes de los partidos políticos o coalición que harán entrega de la urna electrónica con la información correspondiente y recibirán copia de la misma.
- Los funcionarios de la mesa directiva de casilla, bajo su responsabilidad y en compañía de los representantes de los partidos políticos o coalición que deseen hacerlo, harán llegar de inmediato el disquete con los resultados generales de la elección al consejo distrital correspondiente.

1.3. Título Segundo, De los Actos Posteriores a la Jornada Electoral y los Resultados Electorales, Capítulo I De la Recepción de las Urnas Electrónicas y Cómputos Distritales

La recepción de las urnas electrónicas y de los cómputos distritales se harían conforme a lo siguiente:

- La recepción de las urnas electrónicas con los programas informativos estará a cargo del personal designado por los consejos distritales. El secretario ejecutivo y los presidentes de dichos consejos tomarán las medidas necesarias para el resguardo de las urnas electrónicas con los programas informativos, hasta la conclusión del proceso electoral las salvaguardarán y dispondrán su depósito en un lugar en el local del

consejo respectivo, el cual deberá reunir las condiciones de seguridad necesarias, al efecto se dispondrá que se sellen las puertas de acceso en presencia de los representantes de los partidos políticos.

- Los consejeros distritales harán la suma de los resultados del disquete, conforme se vayan recibiendo los resultados contenidos en cada urna electrónica. El presidente del Consejo Distrital dará lectura en voz alta en primer lugar a los resultados de la elección de Jefe de Gobierno, después a los de Jefe Delegacional y por último a los de Diputados a la Asamblea Legislativa, en forma sucesiva hasta su conclusión.
- Una vez realizadas las sumas de cada una de las elecciones, se plasmará el resultado en el acta final de escrutinio y cómputo, así como la relación de escritos de incidentes ocurridos durante la misma; de igual manera, se hará constar en dicha acta las objeciones que hubiese manifestado cualquiera de los representantes de los partidos políticos ante el consejo distrital. Los consejos distritales deberán contar con los recursos humanos, materiales, técnicos y financieros para la realización de los cómputos en forma permanente.

1.4. Título Tercero De las Nulidades, Capítulo I De los Casos de Nulidad

Para el caso de las nulidades se tomará en cuenta lo siguiente:

- Instalar la casilla o realizar la impresión del acta comprobante de los resultados de escrutinio y cómputo sin causa justificada, en lugar distinto al señalado por el Consejo Distrital correspondiente.
- Entregar sin causa justificada la urna electrónica con los programas informativos correspondientes al Consejo Distrital fuera de los plazos que señala el *Código Electoral del Distrito Federal.*

2. Reformas al *Código Penal para el Distrito Federal*

En materia penal se tendrían que analizar las reformas al *Código Penal para el Distrito Federal* (CPDF), específicamente en su Título Vigésimo Sexto referente a los Delitos contra la democracia electoral, Capítulo Único Delitos Electorales, ya que cambiarían los términos de la documentación

y el material electoral, y estos se consideran elementos que pueden ser causa de que se cometa algún delito contra de la documentación y material electoral. Por ello, se entendería por:

> Urna electrónica, el sistema tecnológico para la emisión del voto ciudadano que se utiliza en los procesos electorales y de participación ciudadana; y
>
> Los programas informativos, constarían de la lista nominal de electores correspondiente a la sección donde se ubica el módulo de la urna electrónica, la información de los emblemas de los partidos políticos, así como los nombres y las fotografías de los candidatos de los mismos en el Distrito Federal, la activación de inicio de operación de la urna electrónica, la activación del procedimiento de cierre de operación de la urna electrónica, la transmisión de los resultados, y la recuperación de datos.

Para el caso de la urna electrónica, los términos: introducción, sustracción, apoderamiento, destrucción o alteración de la documentación y del material electoral, se emplearán los de: alteración de los sistemas informativos, apoderamiento o destrucción ya sea parcial o total de la urna electrónica.

Para los Artículos 352 al 360 del CPDF se debe realizar un profundo análisis en cuanto a la fijación de las sanciones y multas que se deben aplicar en los delitos electorales tipificados como tales, toda vez que ya no se trata de documentación y material electoral, es decir, de papel, recordando que la boleta electoral es un documento oficial considerado tanto por el Instituto Electoral del Distrito Federal como por el Tribunal Electoral del Distrito Federal, y en caso de que se cometa delito alguno contra este documento es causa de una denuncia y un juicio penal en contra de quien resulte responsable, por lo que para el caso de la urna electrónica se debe aplicar la misma regla de la denuncia y el juicio penal, sólo que podría aumentarse la sanción, ya que se trata de un insumo tecnológico que contiene información de carácter oficial, cuyo contenido es responsabilidad de una institución electoral.

Cabe mencionar, que de continuar con el proyecto de la urna electróni ca, se debe elaborar un modelo adecuado a las necesidades que requiere la Ciudad de México para la emisión del voto ciudadano en los procesos electorales y de participación ciudadana, ya que con la utilización de este sistema tecnológico se brinda la confianza, la legalidad y la certeza de que el fraude electoral es nulo. Además de considerar que la ciudadanía está preparada para aplicar este tipo de avances tecnológicos.

3. Conclusiones

a) La presencia de un sistema tecnológico para la emisión del voto ciu - dadano agiliza el desarrollo de un proceso electoral, con lo que se obtienen ventajas tanto para el ciudadano como para la institución encargada de organizarlo. Por ello es necesario discutir aspectos cen - trales como el político, el social, el tecnológico y las reformas ju - rídicas para su adecuada aplicación, de tal modo que se garantice certeza, legalidad y transparencia al momento de que el ciudadano emita su voto.

b) Hoy, el reto del IEDF es renovar el sistema electoral, involucrando más a la sociedad en los asuntos político-electorales, culturales y, espe - cíficamente, en la importancia que tiene el ejercicio del voto en la Ciudad de México con sus características primordiales de ser univer - sal, libre, secreto, directo, personal e intransferible, como una herra - mienta que facilita su emisión, ya que uno de los fines de que el IEDF es llevar a cabo la promoción del voto y coadyuvar en la difusión de la cultura democrática.

c) Los procesos electorales, la participación ciudadana y la responsabili - dad al momento de votar son elementos que existen en una sociedad democrática, ya que sin éstos, la democracia y los valores cívicos no tendrían razón de ser.

BIBLIOGRAFÍA

BECERRA, Ricardo y otros, *La Mecánica del Cambio Político; elecciones, partidos y reformas*, México, Cal y Arena, 2000.

CASTELLANOS Hernández, Eduardo, *Derecho Electoral en México*, México, Trillas, 1999.

COVARRUVIAS Dueñas, José de Jesús, *Derecho Constitucional Electoral*, México, Porrúa, 2002.

GÓMEZ Orozco, Javier, *Estudios Electorales*, México, Porrúa, 1999.

GONZÁLEZ DE LA VEGA, René, *Derecho Penal Electoral*, México, Porrúa, 2001.

PATIÑO Camarena, Javier, *Derecho Electoral Mexicano*, México, Constitucionalista, 1994.

LEGISLACIÓN

Constitución Política de los Estados Unidos Mexicanos.
Estatuto de Gobierno del Distrito Federal.
Código Electoral del Distrito Federal.
Código Penal para el Distrito Federal.

La urna electrónica: avances y prospectivas

María de los Angeles Fromow Rangel
Fiscal Especializada para la Atención de Delitos Electorales
Procuraduría General de la República

Es licenciada en Derecho por la Universidad Nacional Autónoma de México (UNAM); estudió la Maestría en Tributación Fiscal en el Centro de Estudios Financieros de Madrid, y el Doctorado en Derecho Administrativo en la Universidad Complutense de Madrid, donde obtuvo el grado *Apto Cum Laude* por unanimidad.

En la docencia tiene amplia experiencia como titular de las materias de Derecho Administrativo y Derecho Fiscal en la Facultad de Derecho de la UNAM. Cuenta con conocimientos en reingeniería en procesos y mejora continúa, reestructuraciones orgánicas y financieras con el fin de crear organizaciones más eficaces y eficientes. Desde el 1 de febrero de 2001 se desempeña como Fiscal Especializada para la Atención de Delitos Electorales en la Procuraduría General de la República.

RESUMEN

Esta ponencia presenta un análisis jurídico sobre el marco legal de aplicación que en materia penal federal tiene el voto electrónico, así como los casos en México en los que se ha puesto en práctica la urna electrónica de manera experimental, paralelamente a la realización de ciertos procesos electorales. También aborda las connotaciones legales a considerar en la implementación del voto electrónico, y ofrece una prospección en cuanto a su utilización en nuestro país.

INTRODUCCIÓN

Actualmente los avances tecnológicos en informática y computación inciden de manera notable en nuestras formas tradicionales de hacer las cosas.

Los diseños de programas y equipos de cómputo se desarrollan a un ritmo acelerado y son cada día más sofisticados e indispensables en la vida cotidiana de los países industrializados.

Es a medida que esta tecnología avanza que los organismos electorales aplican distintas innovaciones a la administración electoral, de ahí que la computadora sirva de base para la creación de prototipos en la implementación de la votación electrónica.

En la mayoría de los países que tienen un régimen democrático como forma de organización política, la utilización de nuevos instrumentos y procedimientos para la recepción del sufragio durante la jornada electoral (como el voto electrónico) ha cobrando relevancia, ya que desde hace varios años, el voto electrónico es una realidad en países como Francia, Alemania, Inglaterra, España, India, Brasil, Argentina y Venezuela; los cuales han desarrollado sistemas de votación electrónica empleando instrumentos diversos.

El concepto de *voto electrónico* implica un dispositivo de escrutinio y cómputo de votos con una amplia posibilidad en cuanto al uso de tecnologías y puede asumir gran cantidad de formas, desde el uso de teléfonos celulares, cajeros automáticos y teléfonos convencionales hasta Internet.

Recientes investigaciones realizadas por el Instituto Electoral del Distrito Federal (IEDF) reportan cinco tipos de herramientas tecnológicas para el ejercicio del voto, utilizadas por los países en que los se ha incorpado el voto automatizado: la urna electrónica, las pantallas sensitivas (*Touch Screen*), el contador de votos (escáner), el voto por teléfono y el voto por Internet.

1. Marco legal de aplicación del voto electrónico en materia penal federal

El proceso de democratización en nuestro país se ha forjado a lo largo de los años y, paulatinamente, se ha consolidado una cultura de la legalidad electoral entre los partidos políticos y la ciudadanía.

De tal suerte que, la realidad política de México exige hoy procesos electorales transparentes, apegados a la ley, sin margen para la falta de eficacia, credibilidad, certidumbre y legitimidad de las instituciones democráticas, de ahí que las normas jurídicas deban reflejar la vida de los ciudadanos en los diversos órdenes en los que tiene injerencia.

En este marco, la Procuraduría General de la República (PGR) tiene entre sus responsabilidades la de investigar los delitos federales, que incluyen los de naturaleza electoral, con la finalidad no sólo de perseguirlos, sino también de prevenirlos. De esta manera, a través de la Fiscalía Especializada para la Atención de Delitos Electorales, se vela por la efectividad del voto y se fortalece la cultura de la legalidad de los mexicanos.

Así, en el capítulo único del título vigésimo cuarto del *Código Penal Federal,* en los Artículos del 403 al 408 y el 411 y 412 se establecen los tipos penales en materia electoral.

El marco legal de aplicación en materia penal federal, que proporciona seguridad jurídica ante la emisión del sufragio por la vía electrónica, se circunscribe a las siguientes disposiciones legales: Artículos 401, fracción VI; 403, fracciones IV y VII; 405, fracciones III y IV; y 406, fracciones III y IV.

- El Artículo 401, en su fracción VI, en atención a la urna como aquel material electoral que sufre el acto o conducta considerada como delito.
- La fracción IV del Artículo 403 establece como sanción de 10 a 100 días multa y prisión de seis meses a tres años, a quien obstaculice o interfiera dolosamente el desarrollo normal de las votaciones, el escrutinio y cómputo. La fracción VII de dicho artículo establece la misma punición a quien el día de la jornada electoral viole, de cualquier manera, el derecho del ciudadano a emitir su voto en secreto.
- El Artículo 405 dispone que se impondrá sanción de 50 a 200 días de multa y prisión de dos a seis años, al funcionario electoral que obstruya el desarrollo normal de la votación sin mediar causa justificada, o bien, que altere los resultados electorales, sustraiga o destruya documentos o materiales electorales.
- El Artículo 406 dispone que el funcionario partidista o candidato que sustraiga, destruya, altere o haga uso indebido de documentos o materiales electorales y obstaculice el desarrollo normal de la votación o de los actos posteriores a la misma, se impondrán de 100 a 200 días de multa y prisión de uno a seis años.
- El título noveno del mismo ordenamiento legal, en el capítulo segundo relativo al acceso ilícito a sistemas y equipos de informática en el

> Artículo 211 Bis 2 establece que al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de 200 a 600 días de multa.

Como podemos apreciar, la norma jurídica es dinámica, y debe atender a las necesidades de la sociedad. La ciudadanía reclama estructuras legales que garanticen el ejercicio de los derechos democráticos, figuras que acoten cualquier desviación del ejercicio del servicio público y que además establezcan un marco en el cual actúen los partidos políticos y sus candidatos.

La tarea de procuración de justicia en materia electoral exige una constante revisión y actualización de los preceptos legales que salvaguardan los distintos bienes jurídicos protegidos en los procesos electorales, que sustentan nuestra vida democrática.

2. Algunos avances respecto de la implementación de la urna electrónica en México

El fortalecimiento de la democracia y la profesionalización del personal de las instituciones electorales en México han obligado a éstas a buscar nuevas formas de organizar las elecciones utilizando tecnologías apropiadas a las necesidades del país.

Hoy, pensar en organizar un proceso electoral sin el uso de equipos y sistemas informáticos y de telecomunicaciones resulta imposible. Quizá, los programas de resultados preliminares son el mejor ejemplo de la aplicación exitosa de nuevas tecnologías en este tipo de procesos.

Por ello, el Instituto Federal Electoral (IFE) y los institutos electorales de varios estados de la República como Coahuila, Nuevo León, San Luis Potosí, Distrito Federal y Jalisco, se han interesado en contar con un prototipo de votación electrónica en el que se tomen elementos del modelo tradicional de votación y lo ha puesto en práctica, mediante ejercicios, paralelamente a las elecciones estatales.

3. El IFE

El IFE diseñó un modelo para recibir y transmitir el voto por medios electrónicos, el cual busca reducir el costo de las elecciones, atender la heterogeneidad social y la complejidad geográfica del país, y garantizar la igualdad de acceso para los electores.

Dicho prototipo fue presentado a los integrantes de la Junta General Ejecutiva del IFE por el director de Organización Electoral, Jaime Rivera Velásquez, quien manifestó que el objetivo era tener un medio electrónico para recibir, computar y transmitir los votos de los ciudadanos, el cual al tiempo de preservar los principios de legalidad y certeza, garantice la igualdad en el ejercicio del sufragio, así como propicie, a mediano plazo, una reducción en el costo de las elecciones.

Sin embargo, Rivera Velásquez reconoció que existen diversos problemas como el llenado de actas de casilla, la anulación de votos por error y el traslado de la documentación electoral, que aun cuando no ponen en duda la limpieza de las elecciones, sí son susceptibles de superarse para mejorar la calidad de los procesos electorales.

4. En los estados

Con carácter de prueba, en 2003 se efectuaron ejercicios de voto electrónico en Coahuila, Nuevo León, San Luis Potosí y el Distrito Federal, a continuación se presentan algunas características de los equipos utilizados en ellos.

Coahuila

Homero Ramos Gloria, presidente del Instituto Electoral y de Participación Ciudadana de Coahuila expresó que el prototipo de votación electrónica, que se utilizó en este estado, retoma elementos del modelo tradicional de votación, elimina la utilización física de boletas y actas electorales, suprime el recuento de boletas depositadas en las urnas tradicionales, agiliza la entrega de resultados definitivos y reduce considerablemente los costos financieros, obteniendo así mayor certeza en los resultados de votación.

El sistema de recepción del voto implementado en Coahuila funciona de manera fácil y no requiere la capacitación especializada del elector,

ya que su manejo es básicamente mediante el tacto, y los elementos audiovisuales guían al elector para que, mediante pasos sencillos, éste emita su voto.

Una característica del sistema de votación electrónica es su manejo individualizado, ya que está diseñado para utilizarse en cada casilla sin tener ningún vínculo de comunicación con otras, lo que garantiza que la recepción y cómputo de la votación sean únicos en cada casilla, además dichos procedimientos se realizan invariablemente con la vigilancia permanente de los funcionarios electorales y de los representantes de los partidos políticos.

La manera de ingresar al sistema para emitir el sufragio es por medio de una tarjeta especial que contiene un código de acceso, el cual ha sido generado aleatoriamente y codificado con un esquema de seguridad que no permite descifrar la información contenida en ella. Las tarjetas están diseñadas para ser utilizadas únicamente en la urna electrónica de una casilla determinada y por una sola ocasión.

El sistema de recepción del voto (urna electrónica) tiene una pantalla sensible al tacto que permite al elector, una vez verificado el código de acceso correspondiente, acceder a la boleta virtual para que realice con mayor seguridad y certeza la elección de su preferencia.

El voto electrónico contempla un sistema a prueba de fraude, toda vez que la información queda resguardada en cuatro diferentes formas auditables que imposibilita el fraude electrónico: el propio sistema, el medio magnético removible, la copia de seguridad impresa y la urna convencional donde los electores depositan los comprobantes impresos.

Otra característica de este sistema es la garantía de su inviolabilidad, ya que únicamente se puede operar mediante dos códigos especiales, uno de inicialización y otro de cierre, códigos que estarán exclusivamente en poder de la persona que funja como presidente de la mesa directiva de casilla.

Aunado a ello, el sistema conserva y garantiza las características fundamentales del sufragio como es el derecho universal, cuyo ejercicio es libre, secreto y directo.

Nuevo León

En Nuevo León, el 6 de julio de 2003, además de las 4 600 casillas instaladas en las elecciones estatales para elegir gobernador y presidentes municipales, se instalaron 115 más en lugares estratégicos donde los ciudadanos pudieron realizar el ejercicio de votar de manera electrónica sin alterar los resultados de la votación oficial.

Pablo Longoria, comisionado ciudadano del consejo estatal electoral en esa entidad federativa expresó que se buscaba que la gente experimentara la urna electrónica, para poder saber cómo se sentían votando de una forma y de otra; además de contrastar la velocidad de los resultados y la veracidad de los mismos.

San Luis Potosí

San Luis Potosí se sumó a las iniciativas del voto electrónico de otros estados, y el presidente del consejo estatal electoral, Juan Dibildox Martínez, presentó el 9 de octubre de 2002 la forma en que operarían las urnas electrónicas para los comicios de 2003, particularmente en las zonas donde no había energía eléctrica, y comentó la pretensión de distribuir 30 más en el estado para hacer una prueba.

Estas urnas, comentó el funcionario estatal, contaban con un sistema que podría operar con un acumulador de celdas solares y una batería.

Distrito Federal

El IEDF también presentó un proyecto de automatización del voto para la elección de representantes populares de 2003. En este proyecto se realizó un simulacro con el uso de 50 urnas electrónicas distribuidas en cada uno de los distritos uninominales en los que se divide el Distrito Federal.

En el simulacro participaron diversas empresas nacionales y extranjeras que ofrecieron valiosos productos para sustituir el voto manual por su automatización. Empresas españolas, estadounidenses, brasileñas y mexicanas presentaron equipos con una variada composición tecnológica, cuyos costos fueron desde 400 dólares (que los brasileños usan con una vida útil estimada en 14 años, es decir, equipos que durarían más de tres períodos electorales), hasta equipos de 6 mil dólares.

Para Eduardo R. Huchim, consejero electoral del IEDF, técnicamente, la urna electrónica es un instrumento confiable que no tiene problemas y, según refirió, si se detectara alguno en las pruebas, sería resuelto fácil y rápidamente por la versatilidad de los prototipos que existen en el mercado.

Agregó que proveedores como la española Indra, la estadounidense Diebold y las mexicanas Alta Tecnología e Ingeniería en Procesamiento Digital ofrecen respuesta a todas las "suspicacias", lo mismo contra piratas cibernéticos o *hackers*, que para evitar el "embarazo" de las urnas.

Huchim comentó que la urna electrónica ofrece varias ventajas, entre las que destacan:

a) Rapidez en la obtención y difusión de resultados
b) Aligeramiento de la pesada carga de trabajo de los funcionarios electorales
c) Simplificación de las tareas que se desarrollan en las casillas electorales
d) Ahorros en la documentación y en los materiales electorales

El nuevo mecanismo, a diferencia de la utilización física de boletas y de actas electorales, suprime el recuento de boletas depositadas en las urnas tradicionales, agiliza la entrega de resultados definitivos y reduce costos financieros, lo que hace que se obtenga mayor certeza en los resultados de la votación.

Con el proyecto de la votación electrónica se pretende dar confianza adicional al elector, celeridad a los procesos electorales y absoluta transparencia y certidumbre en cada voto expresado.

No obstante, existe el riesgo de que los procesos electorales puedan ser alterados por desórdenes civiles o sabotajes, por tanto la tecnología seleccionada debe ser lo suficientemente robusta y flexible para funcionar incluso si se presentan dichos problemas.

Por su parte, Leonardo Valdés Zurita, consejero electoral del IEDF dijo que con la urna electrónica terminarían los litigios electorales, toda vez que la votación emitida puede auditarse sin lesionar el carácter secreto del voto.

Con dicha auditoría se garantiza la seguridad y certeza para los ciudadanos que participan en votaciones electrónicas, además los procesos electorales llevan aparejados candados de seguridad vinculados con la integración e impresión de la lista nominal, las boletas electorales y la capacitación de los ciudadanos que fungen como funcionarios de casilla.

Grupos de trabajo

El presidente del Consejo Electoral de Jalisco, Alejandro Elizondo, indicó que en el Primer Encuentro Nacional de Organismos para el Análisis de propuestas de Urna Electrónica, celebrado en julio de 2004, se acordó integrar tres grupos de trabajo para analizar el proyecto de urna electrónica.

Estos grupos de trabajo que son de tipo técnico, financiero y jurídico-político, se encargarán de analizar en cada uno de esos ámbitos dicho proyecto para que en una siguiente reunión del comité técnico se elaborará la propuesta de un modelo nacional de urna electrónica.

Como vemos, los institutos electorales, federal y locales han realizado diversos proyectos para la automatización del voto, sin que a la fecha se haya cristalizado fehacientemente alguno de ellos.

3. El voto electrónico y sus implicaciones legales en materia penal federal

En nuestro país el uso de los recursos informáticos no se ha incorporado plenamente a los procesos a través de los cuales los ciudadanos emiten su sufragio, pues aún se efectúa el escrutinio y cómputo de los votos tanto en las casillas como en los órganos electorales.

Al respecto, como parte de las razones, se aduce que en la legislación electoral no se contempla la realización de estos actos por medio de implementos tecnológicos y por tanto, se preserva el procedimiento tradicional.

Más allá del marco legal actual de aplicación en el ámbito penal electoral federal, habría que considerar las implicaciones jurídicas que conlleva la emisión del sufragio a través de medios electrónicos.

Así, desde un punto de vista conceptual, tendríamos que empezar por redefinir o establecer lo que debemos entender lo que sería la urna electrónica en el marco específico de los materiales electorales.

Por otro lado, en cuanto al contexto social, en tanto que en el uso de nuevas tecnologías estamos en presencia de un cambio de forma en los mecanismos de emisión del sufragio, ello no es óbice para que las viejas o nuevas prácticas de cometer delitos electorales, continúen realizándose.

Esto es, que las disposiciones actuales en materia penal electoral federal, expuestas con antelación, resultan del todo aplicables, pues van dirigidas a las conductas ilícitas, no así a los mecanismos o sistemas, por lo que, sólo se tendría que afinar, el verbo núcleo rector de la acción o conducta cometida.

Además de ello, debemos considerar que en el acto de emitir el voto a través del uso de la tecnología y la comunicación, el bien jurídico tutelado se amplía en atención a ese acto privado e individual, cuya información obtenida parte de la emisión inmaterial de un resultado que es de tipo virtual. De ahí que las conductas de sustraer, destruir, alterar o modificar tendrían que atender a esta forma intangible del resultado.

Por tanto, para garantizar la seguridad jurídica del sufragio frente al impacto de la tecnología y la comunicación, en forma paralela se debe garantizar la salvaguarda de esa información, en su anonimato, alteración, modificación y verificación hacia el elector.

Otra de las implicaciones que debemos tomar en cuenta en la implementación del voto electrónico es el ámbito de competencia para la aplicación de la ley, ya que no podemos soslayar el voto de los mexicanos en el extranjero, por lo que es necesario referir el Artículo 2° del *Código Penal Federal*, que literalmente establece: "por los delitos que se inicien, preparen o cometan en el extranjero, cuando produzcan o se pretenda que tengan efectos en el territorio de la República;". Lo anterior es el fundamento legal para la aplicación de dicho código punitivo a los delitos electorales, cometidos por mexicanos o extranjeros fuera del territorio nacional y en contra de los bienes jurídicos tutelados por el Estado mexicano; por consiguiente, dicho instrumento legal es aplicable para punir conductas típicas, antijurídicas y culpables en materia electoral federal.

En el contexto actual es posible la persecución por parte de la Representación Social de la Federación de un delito electoral, por ejemplo, en los casos de autoría mediata, instigación o complicidad, en que el autor mediato, el instigador o el cómplice, respectivamente, de algún delito electoral se encuentran en otro estado de la República o en territorio extranjero, en esa hipótesis, es perfectamente posible ejercitar acción penal, por alguno de los tipos penales en materia electoral. Estas implicaciones dogmáticas se vislumbran tratándose de los autores directos y de los coautores, al no existir las condiciones de tiempo, modo, lugar y ocasión que requieren la mayoría de los tipos penales en materia penal electoral.

En materia adjetiva, la situación no cambia, pues el Artículo 7° del *Código Federal de Procedimientos Penales*, dispone: "En los casos de los Artículos 2, 4 y 5, fracción V, del código penal, será competente el tribunal en cuya jurisdicción territorial se encuentre el inculpado; pero si este se hallare en el extranjero lo será para solicitar la extradición, instruir y fallar el proceso, el tribunal de igual categoría en el Distrito Federal ante quien el ministerio público ejercite la acción penal."

Ante esto, también es competente para conocer de los delitos electorales federales cometidos en otro estado de la República o en el extranjero, el Poder Judicial de la Federación a través de los juzgados de distrito. Por lo cual, el tratamiento procesal de los asuntos no presenta ningún tipo de variante, respecto de los delitos cometidos en territorio nacional, ya que para cuando el juez ejerza su competencia, esto será, una vez integrada la averiguación previa y, por ende, salvado el conflicto de competencia.

5. Prospectivas del voto electrónico en México

Existen varias empresas, nacionales e internacionales, que ofrecen propuestas y soluciones para la emisión del voto electrónico en México, las cuales, aunque resultan operativas, lo son solamente en escenarios reducidos y controlados. Y es que los problemas de seguridad y confianza que generan ciertos temores, incertidumbre y dudas, debido al estado actual de la tecnología, resultan por ahora insalvables.

Los sistemas de votación electrónica propuestos hasta la fecha en el contexto de las nuevas tecnologías, no obstante las ventajas que ofrecen

de simplificación del procedimiento, de la omisión del escrutinio, de la precisión y la celeridad en los resultados, y la existencia de errores y omisiones, entre otras, no han podido solucionar los retos técnicos y sociopolíticos, pues todavía ninguna empresa o gobierno han podido sortear sus dificultades de manera completa y cerrada.

Citemos como ejemplo la experiencia de los Estados Unidos, en donde la mayoría de universidades se han unido para denunciar las prácticas fraudulentas de la firma de voto electrónico, Diebold Electronics Systems, ya que un *hacker* entró en el sistema de esta compañía y copió 15 mil documentos confidenciales, con lo que se pudo demostrar que el *software* usado en las elecciones por dicha empresa, (que dio la victoria a Bush y Schwazeneger), tenía agujeros que permitían cambiar los votos.

De la revisión que se hizo a los documentos internos de Diebold Electronics Systems se demostró que esta empresa conocía los graves errores de seguridad en sus programas, que estos podían provocar fraude, como la posibilidad de cambiar votos sin dejar rastro o la instalación de programas no certificados por las autoridades electorales.

Las consecuencias no se hicieron esperar y se anunció que se retrasaría la certificación de los productos de Diebold para las elecciones de 2004, hasta que no se haga una investigación.

Por otro lado, Mark Fleisher, presidente del Partido Demócrata de Arizona, mostró su confianza en que los próximos comicios presidenciales estadounidenses "cederán protagonismo a Internet", y señaló los considerables aumentos en la participación del electorado que consiguió su formación en marzo de 2003 con la celebración de sus elecciones primarias en Internet y al estilo tradicional, simultáneamente.

Sin embargo, existe escepticismo en cuanto al uso de tecnologías como el Internet, que no garantiza el anonimato, ni la seguridad, ni la formación política del electorado, lo cual se funda en la existencia de los *hackers*. Tales factores dificultan que el entorno de los procesos electorales tenga visos de una efectiva democracia.

Como resultado de esto ha surgido un debate público sobre la seguridad del voto, en torno a la cual se ha creado una plataforma para exigir su fiabilidad y como resultado de ello, en julio de 2004, cientos de

miles de personas participaron en una jornada de protesta en 24 ciudades de Estados Unidos contra el uso de lo que calificaron máquinas de votación computarizadas "sin verificación", que se podrían utilizar en la elección presidencial de noviembre.

Sin embargo, los fabricantes de las urnas electrónicas insisten en que éstas son más confiables que otros sistemas, pero una serie de errores en la votación por correo electrónico ha llevado a los manifestantes a buscar salvaguardas. Según algunas estimaciones, unos 50 millones de votantes podrían utilizar la nueva tecnología en la elección del 12 de noviembre.

En México, Luis Carlos Ugalde, consejero presidente del IFE ha señalado que el proyecto de la urna electrónica es una idea que se analiza para el futuro, y no sería sino hasta dentro de una década que se pueda implementar su uso en el ámbito federal, de ahí que se descarte su uso para las elecciones de 2006 y seguramente para la elección legislativa de 2009, aunque probablemente en las elecciones locales se establecerá en un periodo más breve.

6. Conclusión

Políticos y analistas coinciden en expresar que la mayor preocupación que suscita el voto electrónico es la seguridad. Seguridad que tiene que ver más con aspectos de carácter tecnológico, que de tipo legal.

Por ello, aun cuando para muchos la panacea es el voto electrónico, su implementación no reviste sólo un problema tecnológico, sino financiero, demográfico y cultural, pero especialmente su estructuración jurídica en los distintos campos se hará necesaria una vez que se sienten las bases y sus mecanismos, es decir, una vez que se decidan las formas de su implantación, y será entonces que entraremos a un debate de cómo legislar en esta materia.

Las nuevas tecnologías en la democracia

Julio Téllez Valdés
Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM)

Doctor en Derecho y profesor investigador de tiempo completo en el Departamento de Derecho del ITESM, campus Estado de México.

Gabriela Grande Patiño
ITESM

Licenciada en Derecho y profesionista de Apoyo en el ITESM, campus Estado de México.

RESUMEN

Una democracia apoyada en las tecnologías de la información y de la comunicación, también sirve para legitimar decisiones que representan los derechos y las obligaciones constitucionales.

La forma nunca será el fondo, pero sí depende de la forma (correctamente estructurada, organizada, planeada y reglamentada) dar confianza y garantía a los ciudadanos de que los procesos electorales que involucran máquinas también brindan facilidad, rapidez y confidencialidad.

INTRODUCCIÓN

Aspectos jurídicos en el uso de urnas electrónicas.

La Democracia no es solamente una estructura jurídica y un régimen político, es sobre todo un sistema de vida fundado en el constante mejoramiento económico, social y cultural del pueblo que sirve para resolver los problemas pacíficamente.

La *Constitución Política de los Estados Unidos Mexicanos* menciona que son los ciudadanos quienes están obligados a votar en las elecciones populares, que tienen el derecho de poder ser votados para todos los

cargos de elección popular y ser nombrados para cualquier empleo o comisión, conforme a las calidades que establece la ley.

En nuestra Constitución se establece que tienen la calidad de mexicanos los varones y mujeres que hayan cumplido 18 años, y que tengan un modo honesto de vivir.

1. Consideraciones para la utilización de tecnologías de la información y de comunicación

Se debe establecer una conjunción de datos (bases de datos) que ayuden a identificar qué persona puede votar, para así permitirle el acceso con facilidad.

Entonces para formar la base de datos debe considerarse:

- Su inscripción (conocer, modificar y cancelar datos).
- Reconocimiento oficial (reglamentaciones y procedimientos sobre el manejo de información).
- Garantizar el derecho a la privacidad, que implica recibir información de bases de datos especificando finalidad, contenidos, responsables, sesiones, publicación, acceso para verificar, subsanar o suprimir datos; impedir registro, grabación o copiado, conservación, extracción, uso, comunicación, manipulación y procesamiento sin consentimiento libre, consciente y expreso.

Algunos de los aparatos o máquinas electorales electrónicas y procesos que se han empleado en las elecciones utilizando las tecnologías de información y comunicación son los siguientes:

1) *Cazahuellas* que construyen bases de datos de huellas digitalizadas de los ciudadanos cuando éstos ejercen el derecho al voto.
2) Urnas con las listas nominales, sólo del distrito correspondiente y una tarjeta de memoria que registra las respuestas.
3) El ciudadano se identifica con su credencial de elector, la pantalla de la urna despliega un mensaje de bienvenida y después de oprimir

un botón verde inicia la selección, se le solicita confirmar la opción elegida para continuar y así sucesivamente.

4) Mampara y urna electrónica con tarjeta de memoria que contabiliza los votos e imprime un acta (documento legal de la casilla) y guarda información en un soporte magnético que se entrega en la central donde se ubique la computadora que reconocerá el sistema validando los datos sin decodificarlos para subirlos a una red vía telefónica que llegará a un servidor, el cual desencriptará los resultados.

5) El elector ingresa a una página de Internet en una computadora disponible el día de la votación, en cierto horario con una clave (después del tercer error se bloquea el sistema), en la boleta están los logotipos de los partidos políticos o de las coaliciones contendientes y una vez hecha la elección, dando doble clic, aparecerá una foto del candidato para confirmar su voto.

6) Voto electrónico presencial: equipo compacto portátil y ligero, sencillo de instalar; es una estación autónoma de voto, tiene una pantalla a color de 15 pulgadas, con batería, lector de tarjetas y conexión remota para comunicar resultados. El elector se identifica ante el presidente de la mesa directiva de casilla, pasa a la estación autónoma de voto, donde podrá marcar su elección en la pantalla digital con un lápiz óptico integrado.

7) Voto por Internet: Sistema para la emisión del voto a través de una división especializada que resta servicios de captura y gestión de datos a través de un certificado digital que da acceso a una página donde se efectúa la selección a través de un menú, el voto es computado en un servidor central en el momento de llevarse a cabo, y la seguridad e inviolabilidad se cuida trabajando en un área restringida en donde se encuentra el servidor. Cabe aclarar que la información sería enviada en forma encriptada, y sin poder relacionar la identidad del elector con el voto emitido.

8) Escrutinio electrónico: el voto se realiza tradicionalmente en boletas y con una urna tradicional, terminada la votación se pasan las papeletas por el escáner de alta velocidad automatizando el proceso.

9) Sistema Inteligente: tarjeta con banda magnética con un chip computarizado; el elector desliza esta tarjeta por el lector anexado a la terminal la cual revisará que la tarjeta inteligente sea electoral y valide al elector para participar en los comicios. El elector interactúa con la terminal al tocar la pantalla dactilar para hacer su elección y si confirma su voto, éste será guardado y la tarjeta electoral se cancelara para evitar que vuelva a votar con esa misma tarjeta; el elector debe devolver la tarjeta al funcionario de casilla quien la programará nuevamente para el siguiente elector. El funcionario termina el procedimiento de votación al insertar en el administrador una tarjeta final en la terminal y contestar la confirmación de que este procedimiento concluyó. Los resultados son guardados en una memoria magnética y sólo se transmiten electrónicamente al servidor.

2. Aplicación de la tecnología de la información y de comunicación

Algunos procesos de toma de decisiones donde se ha aplicado esta tecnología son los siguientes:

- Venezuela en el referéndum de Hugo Chávez para que éste continuara, o no, en la presidencia. El 18 de agosto de 2004 se emplearon las urnas tradicionales y electrónicas contando con un grado de participación extraordinario de 94.49 por ciento.
- México, en el Distrito Federal, paralelamente al voto de forma tradicional, en las elecciones de 2003 el IEDF instaló 150 urnas que mediante un convenio con el Tribunal Electoral de Brasil obtuvo en calidad del préstamo, y además recibió asesoría técnica en cuanto al *software*.
- México, en Nuevo León, en las elecciones de julio de 2003 para renovar al gobernador del estado, los ayuntamientos y el Congreso Local se usaron urnas con lector óptico para detectar los datos de la boleta.
- México, en San Luis Potosí, se presentó una iniciativa ante el Consejo Estatal Electoral en octubre de 2001, con el propósito de utilizar 30 urnas electrónicas con celdas de energía solar o pila recargable a

efecto de ser usadas incluso en zonas donde no se contaba con infraestructura eléctrica.

- México, en Baja California, el Consejo Estatal Electoral a través de la Dirección General de Organización Electoral elabora un proyecto con el propósito de facilitar y hacer eficiente la jornada electoral con nuevas tecnologías sin afectar su autenticidad y confidencialidad.
- México, en Coahuila, en sus elecciones de septiembre de 2006 harán uso de urnas electrónicas
- Australia, se emplearon tarjetas magnéticas de identificación para elegir a los parlamentarios en octubre de 2001 y de 2004.
- Estados Unidos (EU), en 2004, se utilizaron tarjetas inteligentes que contienen un chip, en las elecciones presidenciales.
- España, Madrid en 2003 con el ejemplo más reciente en el ejercicio de consulta ciudadana denominado "MadridParticipa".

3. Retos para el empleo de urna electrónica

Algunos de los problemas que se han presentado o que se podrían presentar al utilizar urnas electrónicas son los siguientes:

1. La efectividad de las máquinas (fallas no solucionables inmediatamente).
2. La instalación (acceso a medios tecnológicos) y funcionamiento de los equipos.
3. Que la logística no afecte el tiempo empleado en votar.
4. La violación de confidencialidad (*hackers* o *crackers* que pretendan intervenir en el proceso o en el resultado) que pudiera derivar en un fraude electoral.
5. Que las empresas garanticen un servicio confiable de transmisión de información en telecomunicaciones.
6. La capacitación al personal de soporte técnico.
7. Determinar las empresas que programen o creen dichas urnas.
8. El financiamiento (el gasto en documentación y material electoral).
9. La sustitución de los miembros de la mesa directiva de casilla.

10. La desconfianza, tanto de los partidos políticos y principalmente de los electores en cuanto el uso de estas tecnologías en un proceso tan significativo como lo es el electoral.
11. Que las tarjetas inteligentes sean accesibles en el mercado tanto por su localización como por su precio, y si una persona conoce el protocolo puede implementarlo y poner en duda su legitimidad.
12. El desvió y uso inadecuado de la información de los electores a través de personas especializadas en el manejo de equipos automatizados *(hackers)* como ha sucedido en Estados Unidos.

Lejos de abarcar toda la problemática que implica la aplicación de las nuevas tecnologías en los procesos electorales, a continuación planteamos algunas soluciones posibles, que de manera enunciativa y no limitativa, podrían aplicarse:

1. Si se debe reparar o sustituir un equipo y no se puede, se procede manualmente con funcionarios de la mesa directiva de casilla, los cuales deben contar con suficientes tarjetas manuales para cubrir la demanda. Las fallas que se presenten pueden ser por: interrupción por causa mecánica de la votación, interrupción de transmisión de información y escrutinio, y totalización de la información. Si fallan las máquinas en el proceso de verificación, puede encontrarse la diferencia entre los resultados de las máquinas y los del conteo manual, considerando una diferencia prior para poder validar la transparencia del proceso.
2. Cuidar la descentralización (respetar la estructura divisional de distritos y no conjuntar todo en un mismo punto sino apoyarse en un sistema horizontal); los servidores replicados (en constante comunicación para evitar problemas de seguridad o sobrecarga y confiabilidad); el sistema de recuento con recepción de información en tiempo real con protección y recuperación ante fallos.
3. Captar huellas al final del procedimiento de votación para evitar pérdida de tiempo.
4. Presentar una campaña masiva y sostenida de información por el tiempo necesario, además de un sistema de certificación electrónica con

firmas y certificados digitales con realimentación al usuario mediante un correo electrónico encriptado y sistemas de doble clave para registro y emisión de voto (que permite garantizar que somos quienes emitimos el voto), es decir, buscar en todo momento la confiabilidad.

5. En caso de faltar alguno de los funcionarios de la mesa directiva de casilla, éstos podrán ser sustituidos por suplentes escogidos por sorteo y no designados previamente.
6. Verificar los resultados.

Es indispensable recalcar el hecho de que lo antes mencionado implica delimitar los parámetros sobre los que se desarrollará dicho proceso.

Los puntos importantes que no podemos olvidar si queremos procesos electorales, legítimos, confiables, responsables, garantizando los derechos y las obligaciones constitucionales son:

- Acceso pleno a la libertad de información, lo cual considera libertad para el ejercicio del voto (sistema o *software* libre y gratuito), para la orientación del voto, y de información antes, durante y después del ejercicio del voto, como conocer *a priori* cuestiones consultadas, las opciones de elección, el proceso, así como tener conocimiento de los presupuestos e implicaciones.
- La recopilación de datos a través de un registro con formularios e inscripción gratuita con un protocolo: codificación de contraseñas, *backup* y recuperación registro de incidencias.
- Contar con un manual de procedimientos.
- Condiciones mínimas de privacidad y seguridad.
- Responsables y responsabilidades plenamente establecidas.
- La protección contra el uso indebido de datos de los electores.
- Presencia de observadores internacionales garantizando la imparcialidad, objetividad, credibilidad, confianza y transparencia, situación que puede brindar confianza al mismo proceso.

Las facilidades y optimizaciones de las tecnologías de la información y de la comunicación en materia electoral, pueden ser un buen impulso para la aplicación de las innovaciones, como las siguientes:

1. Disminuir el trabajo de funcionarios electorales, simplificar las tareas en casillas, aumentar la rapidez en el conteo y en la difusión de resultados, generar ahorros en documentación y material electoral, además de disminuir el margen de error y la corrección de situaciones como votos nulos o inválidos.
2. Reducir los recursos financieros que se destinan a los procesos de elección a mediano y largo plazo.
3. Ofrecer el uso de tecnología en zonas donde no hay energía eléctrica, a través de fuentes anexas como el acumulador con celdas de energía solar o baterías.
4. Otorgar legitimación de nuestras decisiones; esto no quiere decir que las computadoras tomen las decisiones sino que le dan validez y aceptación a las decisiones por parte de la sociedad, brindando autenticidad.
5. Hacer un proceso más simple y amigable para el elector.
6. Permitir la inviolabilidad de la información por medio de la encriptación, garantizando su privacidad.
7. Favorecer el incremento del número de votos, porque se votaría desde cualquier punto, aunque esto no quiere decir que disminuiría de inmediato (pero sí a la larga) el grave problema del abstencionismo o la indiferencia social.
8. Facilitar la participación de personas con capacidades diferentes.

La incorporación de estas tecnologías en un proceso electoral es un paso más en la evolución de la sociedad.

La tecnología cada vez se va involucrando e incorporando en nuestra actividad cotidiana y no podemos soslayar este hecho, e incluso podríamos pensar en extenderlo al periodo de campañas (sistemas de programación de medios de comunicación masiva, sistemas de audiencia activos y sistemas cualificados que corren en tiempo real).

4. Consideraciones finales

La democracia es una manera pacífica de resolver los conflictos con la visión de fortalecer el pacto social y la gobernabilidad, pues de lo contrario se padecería un incalculable costo político. Esta actividad debe ser apoyada y robustecida por los partidos políticos, las autoridades y los ciudadanos, ya que somos nosotros quienes construimos la estabilidad del Gobierno y el Estado de Derecho.

Son precisamente las instituciones democráticas las que deben facilitar la participación plena de todos los ciudadanos, sean mayorías o minorías, sobre todo porque los resultados electorales se convierten en decisiones constitucionales.

La integridad de la elección es básica para la integridad misma de la democracia. La transparencia y la comprensión son fundamentales para los electores y para los candidatos, de tal manera que cuando se apliquen modos diferentes de elegir a nuestras autoridades, no se ponga en duda la legitimidad de éstas.

El uso extendido de las tecnologías de la información y de la comunicación es la clave para tener un voto de confianza, al facilitar el avance de los derechos civiles y de la vida democrática y en nuestro país.

FUENTES DOCUMENTALES IMPRESAS O ELECTRÓNICAS CONSULTADAS

Instituto Electoral Veracruzano, "Dossier sobre el Voto Electrónico", *Revista Cultura Democrática*, México, Instituto Electoral Veracruzano, marzo 2003, núm.9, pp. 35 a 146.

Téllez Valdés, Julio, "Notas Breves sobre el Voto Electrónico en México", *Revista Nova Luris*, núm. 1, México, ITESM-CEM, pp. 177 a 187.

Cainberra Connect, "Elections Act Home", http://www.elections.act.gov.au

E-Democracia, "Tecnologías sobre el voto electrónico", http://www.edemocracia.com/biblioteca/eVoto/materiales

Electronic Frontier Foundation and Stanford Law Clinic, "Sue Electronic Voting Company", http://www.eff.org/Legal/ISP_liability/OPG_v_Diebold/20031103_eff_pr.php

"Fallos en *software* de voto electrónico en EE.UU", http://www.vsantiviru.com/mm-fallos-voto.htm

FERNÁNDEZ, Gerardo, "Los resultados del RR", http://noticias.eluniversal.com/1004/08/04/opiart04491B.shtml

http//www.reuters.com/news/Article.jhtml:sessionid=FOCLZHHWIC024CRBAEOFEY?type=worldNews&storyID=5986816

http://www.us.terra.wired-com/wired/politica/0.115625063.html

Kuro5hin. "Technology and culture, from the trenches. Diebold Met with Electronic Civil Disobedience", http://www.kuro5hin.org/story/2003/10/21/2367/2543

Observatorio Voto Electrónico, León, España, http://www.votobit.org/

Portal Jurídico del Tecnológico de Monterrey, *Constitución Política de los Estados Unidos Mexicanos*, http://www.cem.itesm.mx/derecho

REVENTÓS, Laia, "Criptografía española para votar por Internet y teléfono móvil", http://www.el pais.es

REVENTÓS, Laia, "La tecnología está preparada para implantar el voto electrónico, pero no la ley". http://www.odec.es/odec/index.php?id=455, mayo 22 de 2003

Robotiker, http://revista.robotiker.com/articulo79/pagina1.jsp

UNIVERSIDAD POLITÉCNICA DE MADRID, http://oasis.dit.upm.es/

"Venezuela estrenó el voto electrónico", http://noticias.arcoiris.tv/modules.php?name=News&file=article&sid=243

"Venezuela: expectativa por veredicto observadores en referendo", http://mx.news.yahoo.com/040816/8/192z4.html

El voto automatizado en el Distrito Federal: Reflexiones para una reforma política en materia electoral

Carlos Albero Díaz González Méndez
Instituto Electoral del Distrito Federal (IEDF)

Licenciado en Sociología por la Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México, y estudiante de la Maestría en Estudios Políticos y Sociales en la misma facultad. Actualmente se desempeña como consejero electoral del Distrito Electoral XXX en el IEDF.

RESUMEN

La ponencia esboza cuatro líneas generales de reflexión en torno al sistema de votación automatizado y su posible implementación en el Distrito Federal, a partir de la experiencia con la prueba piloto de julio de 2003, dichos trazos corresponden a la relación existente entre los elementos económicos, jurídicos y culturales que envuelven el proceso hipotético de votar y participar con un sistema de esta naturaleza.

INTRODUCCIÓN

El presente ensayo forma parte de un proyecto de investigación en proceso cuya intención es aportar a la sociedad capitalina algunas líneas generales que inviten a la reflexión en torno al sistema de votación automatizado y que, desde mi perspectiva, contribuyen al mejoramiento del sistema electoral, y al ahorro considerablemente de tiempo y dinero requeridos en una elección. La intención de esbozar las ventajas que posee la urna electrónica se basa en que su aceptación está en función del conocimiento que el ciudadano obtiene de la información que brindan las autoridades en la materia, de modo que entre mayor sea la calidad y la claridad de la misma, mayor será la confiabilidad; así, lo anterior

permitiría una reforma al marco jurídico actual, pues la apropiación social de la cultura del voto electrónico ocurrirá sólo cuando los diversos elementos tecnológicos, jurídicos y económicos que lo envuelven sean comunes a los capitalinos.

La cultura ciudadana del sufragio contenida en los procesos democráticos en el Distrito Federal, comprendidos como la cadena de hechos que han dotado al ciudadano de los instrumentos jurídico políticos para participar en la vida política de la ciudad, guarda una relación estrecha con cuatro aspectos fundamentales que trataré de explicar.

El primero es el económico, pues para realizar una elección se requiere una inversión cuantiosa por los diversos insumos que se emplean en los procesos electorales y de participación ciudadana, en particular el gasto en la impresión de las boletas, actas de la jornada electoral, de escrutinio y cómputo, etcétera, y que no son utilizados en su totalidad debido a los altos porcentajes de abstencionismo.

El segundo es el político, que evidencia la transformación del sistema electoral mexicano, pues los cambios sufridos desde aquel fraude electoral de 1988, y su superación como hecho histórico, ocasionó en un primer momento la creación del Instituto Federal Electoral (IFE) en 1990, cuya labor garantizó que la transmisión de poderes ocurriera no sólo de manera pacífica y transparente, sino con estricto apego a una nueva ley en la materia.

Producto de la influencia que suscitó la confianza de los ciudadanos y de los partidos políticos depositada en aquel órgano, ocurre en un segundo momento, la reforma política del Distrito Federal. Así, 1997 quedó marcado por la elección del Jefe de Gobierno, y el 2000 por las elecciones de Jefes Delegacionales y de Diputados a la Asamblea Legislativa del Distrito Federal, pero para estas dos últimas la Ciudad de México ya contó con una institución electoral local propia: el Instituto Electoral del Distrito Federal (IEDF).

El tercer aspecto se relaciona con la manera en que vota el ciudadano y el reconocimiento a la credibilidad construida por la labor del IFE y del IEDF, la cual radica en la innovación de los procedimientos y de las técnicas para la organización, dirección, control y validación de los procesos

electorales, que abarcan desde la profesionalización de sus funcionarios hasta la creación de candados para evitar los fraudes electorales (vía la caída del sistema computarizado, o la falsificación de credenciales, boletas, y demás documentación electoral).

El fraude electoral es una preocupación que obliga a ciudadanos, partidos políticos y demás actores a vigilar constantemente el desarrollo de los procesos electorales, y aun cuando los principios de certeza, imparcialidad, legalidad, objetividad, y transparencia disipan al día de hoy la posibilidad de consumar un fraude, la limpieza de las elecciones ha implicado un proceso de mayor inversión de recursos públicos, lo que ha encarecido el costo de la jornada electoral.

En ese sentido existe la probabilidad de elevar hasta tres veces el precio tomando en cuenta que los cargos de elección popular contemplan las figuras de jefe de Gobierno, jefes delegaciones, y diputados locales, a los que les corresponde una boleta por cargo.

El cuarto aspecto se enlaza entre la búsqueda de un sistema que responda a la necesidad de ahorrar los recursos públicos, (sin que se deje de garantizar el voto universal), y la necesidad de una reforma al *Código Electoral del Distrito Federal* (CEDF), que permita canalizar la experiencia de la "Prueba piloto mediante el uso de urnas electrónicas en un simulacro, durante la jornada electoral local del 6 de julio de 2003 en el Distrito Federal", que realizó el IEDF, la que se proyecta como el sistema de votación del futuro próximo.

Por ello abordaré algunos elementos que considero justifican el cambio del sistema de votación actual, al sistema de votación automatizado.

1. Relación dinero-participación ciudadana

Lo primero es determinar que existe una relación entre el dinero invertido en las boletas electorales y la participación ciudadana, veamos:

Para efectos del ensayo, *participar ciudadanamente* significa realizar dos acciones fundamentales: el ejercicio del sufragio, y la disposición y labor desempeñada por los funcionarios de casilla.

En cuanto al primer tipo de participación, la historia reciente de la Ciudad de México exhibe, en la elección de gobernantes y en la utiliza-

ción de alguno de los instrumentos de participación ciudadana, ciclos variantes de abstencionismo, lo que multiplicado por el dinero invertido demuestra un derroche innecesario; por ejemplo: las elecciones de 2000, en las que el número de votos para elegir a diputados de mayoría relativa fue de 4 342 670, esto es 69% de participación, con 30.13 % de abstención de los registrados de la lista nominal,[65] abstencionismo que en el proceso electoral de 2003 aumentó, pues en el mismo tipo de elección el número de votantes disminuyó considerablemente a 2 936 167, esto es 43% de participación, con una abstención de 56.16% de los ciudadanos registrados en la lista nominal.[66]

Otro caso es el plebiscito realizado en el Distrito Federal en el 2002, en el que se sometió a consulta la construcción de los segundos niveles del periférico y el viaducto, en dicho ejercicio el número de ciudadanos con posibilidad de votar, es decir, inscritos en la lista nominal fue de 6 336 261, de los cuales sólo 420 536 acudieron a emitir su voto, esto es 6.4%, con 93.36%[67] restante de abstención, por lo tanto, el gasto mayor en ambos casos lo generaron aquellos que teniendo todo el derecho político no lo ejercieron.

Más allá de las causas que encierra el abstencionismo, llama la atención que los porcentajes de no participación sean elevados, aún en tiempos de elegir a las autoridades locales, de ahí la inquietud de buscar un sistema de votación que, sin dejar de garantizar las características del voto universal, ahorre en la inversión de recursos y que, sin limitar el derecho del ciudadano al voto, atienda la situación de desperdicio del material electoral, pues el abstencionismo seguirá existiendo con una doble consecuencia: el costo político, (que no deja de tener peso para la legitimidad de los candidatos que son electos popularmente), y el costo económico, en tanto que lo invertido y no utilizado jamás se recupera totalmente, pese

[65] Instituto Electoral del Distrito Federal, *Estadística de las Elecciones Locales 2000*, México, IEDF, 2000, p. 517-518.

[66] Instituto Electoral del Distrito Federal, *Estadística de las Elecciones Locales 2003*, México, IEDF, 2000, p. 23-24.

[67] Instituto Electoral del Distrito Federal, *Estadística del Plebiscito 2002*, México, IEDF, 2002, p. 10.

a que los materiales se reciclen y donen a la Comisión Nacional de Libros de Texto Gratuitos; en vez de ello, el recurso económico podría destinarse a otras áreas de mayor provecho.

Debido a que el presupuesto de ingresos y egresos, que se elabora y aprueba año con año por el Congreso General, es característicamente austero y siempre sujeto a la posibilidad de recortes (que dependen de las variables de la política económica del país) es que crece la necesidad por ahorrar los recursos asignados al IEDF, instancia que si bien es de gran trascendencia para la vida democrática de nuestra ciudad, también requiere de una planeación en el corto, mediano y largo plazo en cuanto a la optimización y máximo aprovechamiento de los recursos, en beneficio de la sociedad capitalina.

Por ello, la hipótesis principal de este trabajo descansa en el hecho de que la viabilidad en el uso de un sistema de naturaleza electrónica, reduce en mucho el gasto de los recursos públicos sin dejar de garantizar las características del voto universal (intransferible, personal y secreto), y además del ahorro en los tiempos para el escrutinio y computo, evita los errores frecuentes en el llenado de las actas por parte de los funcionarios de las mesas directivas de casilla; en este sentido, el Grupo de Seguimiento de la Prueba Piloto concluyó entre otros puntos que:

"Con la emisión de los comprobantes de instalación y apertura de la casilla, así como del cierre de la votación y de los resultados de cómputo de los votos se puede sustituir la impresión y llenado de las actas tradicionales, eliminando el margen de error y contribuyendo con ello a una mayor certeza y confiabilidad en una elección".[68]

Es precisamente este margen de error humano, y aquí el segundo tipo de participación ciudadana, que la disposición a la instalación de las mesas sea cada vez menor, pues la renuencia a formar parte del proceso electoral como funcionario se debe entre otros aspectos, a dos importantes:

[68] Instituto Electoral del Distrito Federal, *Informe de Actividades del Grupo de Seguimiento para el Desarrollo de la Prueba Piloto del 6 de julio de 2003*, México, IEDF, 28 de agosto 2003, p. 4.

a) Lo complicado del llenado de las distintas actas utilizadas en la jornada electoral

b) El tiempo que abarca desde la instalación hasta la entrega del paquete al consejo distrital respectivo

Es decir, ambos crean un efecto disuasivo en la participación de quienes podrían realizar las funciones de recepción, escrutinio y cómputo de la elección en una casilla, muy a pesar de la labor titánica de las instancias encargadas del diseño de la capacitación y de la organización electoral, y también de la tarea de los propios instructores y supervisores, que acuden domicilio por domicilio para convencer a los ciudadanos, porque en ellos recae la responsabilidad de integrar las mesas directivas de casilla.

Las experiencias adquiridas en trabajo de campo, de acuerdo a las áreas de responsabilidad respectivas de las figuras de instructor, supervisor y asistente electoral recogen, a través del desarrollo de las distintas etapas del proceso electoral, el sentir de los ciudadanos insaculados y de los funcionarios designados quienes frecuentemente manifiestan su malestar y su negativa de formar parte en un evento de vital importancia para la democracia capitalina.

Este obstáculo no existiría con la urna electrónica, toda vez que como lo demostró la prueba piloto, el tiempo y el esfuerzo requerido a los funcionarios es menor, además de que los cargos de la mesa directiva de casilla se reducirían a dos, porque la facilidad con la que opera la urna permite prescindir del escrutador, quedando sólo un presidente y un secretario, mismos que cumplirían en su totalidad las tareas de la mesa.

Es importante señalar que integrar las mesas directivas de casilla con dos funcionarios también facilitará la notificación y capacitación por los supervisores e instructores asignados a los consejos distritales, hecho que reflejaría ahorro de recursos al IEDF.

Por otro lado, reiterar que la inversión económica en el material electoral fue necesaria para ganar la confianza y credibilidad del sistema electoral y del sistema político en su conjunto es, sin embargo, una situación ya rebasada, y aclaro que no se trata de desaparecer los mecanismos que dan al ciudadano la seguridad de que su voto sea efectivo, sino que

la urna electrónica es la alternativa viable que debe incluirse en las discusiones para la reforma política del Distrito Federal pues hoy representa un hecho sin precedente en la historia electoral del país.

Así, la experiencia con la urna electrónica aplicada en el proceso electoral local de 2003, a manera de prueba piloto, despliega la posibilidad de renovar el sistema electoral.

2. Propuesta de reforma al *Código Electoral del Distrito Federal*

Los planteamientos a la reforma política frecuentemente descansan en aspectos que pretenden modificar las relaciones políticas que componen a las instituciones del Distrito Federal, y que carecerían de sentido si no contemplaran cambiar la legislación en materia electoral, en particular la forma en como se sufraga, se hacen el escrutinio y los cómputos en la jornada electoral, desde la casilla, el distrito electoral, hasta el Consejo General del Instituto.

Aquí es necesario incluir las propuestas para reformar el CEDF, las cuales permitirán el desarrollo del sistema de votación automatizado, desde la etapa previa a la jornada electoral con los Artículos 174 al 179, la etapa del día de la jornada con los Artículos 189 y 191, la del escrutinio y cómputo del 199 al 203, hasta la etapa final y posterior a la jornada electoral con los Artículos 209 al 214.

Los cambios al articulado arriba citado, pueden realizarse hipotéticamente tomando como referencia las urnas electrónicas prestadas por el Tribunal Electoral Superior de Brasil, e imaginando que si el desarrollo de tecnología propia se acerca a la de Brasil, sin la necesidad de pagar por el uso de la patente, será posible contar en un futuro próximo con el sistema de votación automatizado.

3. La experiencia con la urna electrónica

Cabe aclarar que la reforma legal que se concrete no puede justificarse solamente en la experiencia que dejó a los ciudadanos que participaron en la prueba piloto con urnas electrónicas de 2003 y en las conclusiones a las que llegó el IEDF, sino en un análisis de la necesidad institucional de

automatizar el voto y de la cooperación de la sociedad mediante distintos incentivos que pudiera presentar este sistema.

A manera de reseña, la prueba piloto fue un proyecto aprobado por el Consejo General del IEDF el 31 de marzo de 2003, y que para su ejecución el día de la jornada electoral se determinó instalar 120 urnas electrónicas en los 40 distritos electorales del Distrito Federal, y dentro de cada uno se eligieron tres secciones electorales de más de 750 electores que respondieron a tres niveles socioeconómicos, alto, medio y bajo, de forma que los resultados de los cuestionarios de salida aplicados, verificaran la aceptación o rechazo al sistema de votación automatizado en parte de la sociedad capitalina.

Para darle la suficiente legitimidad al proyecto, con miras a una reforma al sistema de votación, se crearon tres grupos de trabajo, el Grupo de Operación, el Grupo Técnico y el Grupo de Seguimiento de la Prueba Piloto, éste ultimo integrado por técnicos capacitados por cada uno de los partidos políticos representados en ese momento ante el Consejo General,[69] junto con los titulares de la Dirección Ejecutiva de Organización Electoral y de la Unidad de Informática del IEDF, quienes fueron responsables de conocer y verificar de forma detallada los trabajos. Sin embargo, la información que permitió que se llegara a las anteriores conclusiones necesita ser divulgada para que los ciudadanos del Distrito Federal se familiaricen con el uso de la urna electrónica y la consideren parte de su cultura democrática.

Dentro de las conclusiones a las que llegó el Grupo de Operación de la Prueba Piloto destacan las siguientes:

- Se conoció la opinión de los partidos políticos y de los ciudadanos del Distrito Federal, sobre el uso y funcionamiento de la urna electrónica como instrumento para ejercer el voto en los procesos electorales y de participación ciudadana.

[69] Estos fueron los partidos políticos: Acción Nacional, Revolucionario Institucional, de la Revolución Democrática, Verde Ecologista de México, de la Sociedad Nacionalista, Alianza Social, México Posible, Liberal Mexicano y Fuerza Ciudadana.

- Se corroboró que emitir el voto a través de la urna electrónica, constituyó para los partidos políticos y los ciudadanos del Distrito Federal, una forma segura y confiable de sufragar.
- Se verificó que, con el uso de la urna electrónica, se mejoraron los tiempos en la votación, cómputo, transmisión y difusión de los resultados electorales.
- Se corroboró que las medidas de seguridad de la urna electrónica garantizaron el secreto del voto y el resguardo de los resultados.
- Se conoció la capacidad de auditabilidad de los equipos y los programas que permiten este tipo de tecnología.[70]

Las dudas más frecuentes que manifestaron los ciudadanos frente a la urna electrónica radican en la garantía de la operación del sistema y de los programas de cómputo que podrían generar suspicacia, cuestión que según el Grupo de Operación se encuentra resuelta pues:

"El voto es intransferible y personal, toda vez que permite la rápida e inequívoca identificación del votante, en virtud de que se incorporó el listado nominal con los datos de los ciudadanos inscritos en las secciones electorales en donde se instalaron las urnas {...}

"Los programas utilizados fueron los correctos y por sus características, permitieron realizar todo tipo de pruebas técnicas, con objeto de garantizar su funcionalidad el 6 de julio.

"Los programas informáticos utilizados en la urna electrónica, permitieron asegurar la integridad de la información a lo largo de diversas etapas de operación {...}

"Cuenta con los mecanismos necesarios para recuperar los datos de la votación de manera íntegra, en los casos de falla o descompostura del equipo. Asimismo permite la comparación de los resultados que se

[70] Instituto Electoral del Distrito Federal, *Informe de Actividades del Grupo de Operación para el Desarrollo de la Prueba Piloto del 6 de julio de 2003*, México, IEDF, 2003, p. 12.

imprimen en las actas que emite cada urna electrónica con respecto a la información resguardada en los dispositivos de las máquinas, misma que es transmitida para llevar a cabo el cómputo total, garantizando con ello su confiabilidad y seguridad."[71]

Por otro lado, una de las características principales que posee la urna electrónica, y por las que su uso ahorrará tiempo y recursos públicos es el hecho de que:

"Facilitó a los ciudadanos del Distrito Federal, emitir sucesivamente su opinión hasta en tres ocasiones con respecto a sus preferencias partidistas, con lo cual se comprueba que es factible votar en más de una elección en una misma sesión...".[72]

Ahora bien, el resultado de los cuestionarios de salida aplicados en la prueba piloto fue favorable, pese a que el universo de estudio se redujo en comparación con el de la lista nominal, es decir, de los 6 697 034 ciudadanos registrados, sólo 22 173 tuvieron acceso y respondieron a las preguntas arrojando los siguientes porcentajes:

El 92.67% se manifestó a favor de que se utilicen urnas electrónicas en la organización de futuros procesos electorales y de participación ciudadana en el Distrito Federal, y solamente 1 633 ciudadanos, lo que representa 7.33 %, no estuvieron de acuerdo con el uso de este tipo de tecnología.[73]

Cabe señalar que la minoría que manifestó no estar de acuerdo con el uso de la urna electrónica, probablemente base su negativa en el hecho de que la información del sistema y los programas de cómputo no tuvieron la difusión y la claridad suficiente sobre la forma en que operan, especialmente en términos de explicar la seguridad y certeza de que no se puede alterar el sentido de la votación bajo ninguna circunstancia.

Si bien el Grupo de Seguimiento coincide con las conclusiones del Grupo de Operación, en el sentido de que la prueba piloto promete modernizar el sistema de votación de manera segura y confiable, al eliminar

[71] *Ibid.* p. 13-14.

[72] *Ibid.* p. 13.

[73] *Ibid.* p. 15.

al máximo los errores humanos que se comenten en los procesos actuales, es necesario continuar con la divulgación de aquellos elementos que en la ciudadanía despiertan sospecha, es decir, cabría la posibilidad de que el IEDF atendiera las dudas más frecuentes, de forma que se geste una cultura del voto automatizado.

4. Consideraciones finales

Respecto a la diferencia con el gasto de recursos públicos, entre el sistema de votación actual y el sistema de votación automatizado, no fue posible comprobar la hipótesis del ahorro en su totalidad, toda vez que las urnas fueron prestadas, y que el diseño de tecnología propia se encuentra hoy en proceso; sin embargo, la inversión económica en la investigación que realiza el IEDF junto con otras instituciones de educación superior, será eso, una inversión y no un gasto, que en el corto mediano y largo plazo se verá reflejado en los diversos ámbitos de la vida democrática de la ciudad.

En lo que se refiere al primer tipo de participación ciudadana, es necesario comprender que el hecho de abstenerse de votar no es un derecho consagrado en la Ley, pero sí representa una alternativa para aquella parte de la sociedad descontenta con el actuar de los partidos políticos y de sus representantes en cargos públicos, situación que rebasa el alto costo político y lleva un costo económico que no tendría que cubrirse si la urna electrónica es aprobada.

Por otro lado, la urna electrónica no puede obligar al ciudadano a votar por algún partido, pensando en aquellos que su deseo e intención clara es anular su voto, o depositarlo en blanco, luego entonces, la urna electrónica tendrá que conservar estas opciones que actualmente el CEDF establece.

Otro de los puntos que se deberá discutir es el de la lista de candidatos a diputados de representación proporcional, ya que en la boleta tradicional aparecen en una lista plurinominal en el anverso, por lo tanto, la urna electrónica deberá tener la capacidad y sencillez de proporcionar al ciudadano la misma información.

En relación con el segundo tipo de participación, los funcionarios de casilla cumplirán con las tareas de la jornada electoral de forma menos

complicada, evitando errores y el desgaste en el escrutinio, cómputo y llenado de las distintas actas que tienen como consecuencia que la disposición a formar parte en otros procesos electorales y de participación ciudadana se vea disminuida; esto es así, aún cuando en cada proceso electoral se realiza el criterio de seleccionar un mes y una letra para insacular a los ciudadanos y posibles funcionarios. Desafortunadamente las malas experiencias vividas como funcionario son transmitidas primero a la familia y después a los vecinos, dada la proximidad de unos con otros en una sección electoral, sobre todo en aquellas en donde se presenta una unidad cultural más arraigada, o por el contrario, donde la atomización entre vecinos dificulta la integración e instalación de las mesas, situación característica de las secciones con población de un alto nivel socio-económico.

Es entonces, que se crea una cultura negativa de la participación, en tanto los ciudadanos hacen suyas las experiencias antes dichas y reproducen falsos valores con los que identifican a los procesos electorales.

La forma de romper con esta dinámica se encuentra en la modernización de los procedimientos electorales, y que como lo señalé en el inicio, la apropiación ciudadana del voto electrónico, necesita de la internalización de los elementos que lo componen, es decir, que para gestar una cultura del voto electrónico es fundamental la aceptación de los ciudadanos.

En ese sentido cabe reconocer la labor que realiza el IEDF para que la población del Distrito Federal conozca y participe en otras pruebas piloto, muestra de ello es el "Proyecto de desarrollo de pruebas piloto con urnas electrónicas en ejercicios de expresión ciudadana" realizado en 160 planteles de educación media superior en el que participaron 56 517 estudiantes que representaron 171 ejercicios, en el periodo del 12 de septiembre al 1 de octubre de 2003.[74]

Las ventajas que implícitamente colaboran para que el sistema de votación automatizado tenga mayor aceptación, radican en el hecho de que la sociedad, tiene cada vez mayor cercanía y familiaridad con los sistemas

[74] Datos tomados de URNA, *Carta Informativa del Instituto Electoral del Distrito Federal*, año 5, núm. 29, México, IEDF, mayo de 2004, p. 10.

electrónicos en la vida cotidiana, es decir, la vida cotidiana en la ciudad permite con frecuencia el contacto con cajeros automáticos de las instituciones bancarias, teléfonos celulares, computadoras, etcétera, y crea un efecto gradual de relación con los ciudadanos.

Referente a lo político, lanza el reto para que los partidos contribuyan con su parte, y concreten con la aspiración de contar con un sistema moderno, confiable y seguro dentro de un nuevo marco jurídico, de ahí que la reforma al CEDF necesite de su voluntad razonada.

En lo que toca a la tecnología, será imprescindible que el IEDF continúe con la congruencia de incluir en el diseño de la urna electrónica los requerimientos de la población discapacitada para que ejerzan su derecho al voto, entre otros el sistema Braille (que se utilizó por primera vez en un ejercicio de participación ciudadana en el Plebiscito de 2002), en forma de mascarilla, al igual que los aditamentos utilizados en la elección 2003 que atendía a las personas en silla de ruedas o limitadas en sus extremidades tanto superiores como inferiores.

De esta forma en una sola inversión, cuyo tiempo de vida útil permanece como incógnita, se estaría evitando el que cada año electoral o ejercicio de participación ciudadana se adaptaran otros materiales electorales, que implicaría entonces sí un gasto no previsto desde el comienzo.

Finalmente este ensayo sienta las bases para seguir con una investigación más amplia que dé cuenta de forma más precisa a las incógnitas que pudieran presentarse en el proceso de desarrollo de un nuevo sistema de votación.

Así, el desarrollo de la investigación subsecuente aportará elementos necesarios para la construcción de políticas encaminadas a fortalecer el sistema electoral, y que ofrezcan respuesta a las interrogantes que arroja su ejercicio.

Traducir las necesidades ciudadanas y de los partidos políticos de conocer, sin dudas, que la garantía de la información de la votación emitida en una urna electrónica, no puede ser previamente cargada modificada o alterada, junto con la compatibilidad con las figuras de revisión, y apelación de los resultados, facilitará su aceptación.

Sabido es que la democracia no comienza ni termina en el momento de depositar el voto en la urna, sin embargo, es imprescindible que los mecanismos que permiten modernizar el sistema de votación recojan, de forma sencilla, clara y con apego a la legalidad, dicha acción.

El proyecto del IEDF se encuentra en la mesa de discusión, y el análisis que resulte deberá, culminar en una reforma al sistema electoral en su conjunto, y con ello servirá de ejemplo a su homólogo federal para dotar de sentido a una reforma del Estado.

REFERENCIAS BIBLIOGRÁFICAS Y HEMEROGRÁFICAS

Instituto Federal Electoral, *Código Federal de Instituciones y Procedimientos electorales, y otros ordenamientos electorales*, México, IFE, 1999.

CÁMARA DE DIPUTADOS, *Constitución Política de los Estados Unidos Mexicanos*, México, LVIII Legislatura, Cámara de Diputados, 2003.

INSTITUTO ELECTORAL DEL DISTRITO FEDERAL, *Código Electoral del Distrito Federal*, México, IEDF, 2000.

_____, *Estadísticas de las Elecciones Locales 2000*, México, IEDF, 2003.

_____, *Estadísticas de las Elecciones Locales 2003*, México, IEDF, 2003.

_____, *Estadística del Plebiscito 2002*, México, IEDF, 2003.

_____, *Informe de Actividades del Grupo de Operación para el desarrollo de la Prueba Piloto del 6 de julio de 2003*, México, IEDF, 2003.

_____, *Informe de Actividades del Grupo de Seguimiento para el desarrollo de la Prueba Piloto del 6 de julio de 2003*, México, IEDF, 2003.

_____, *Informe de Actividades del Grupo Técnico para el desarrollo de la Prueba Piloto del 6 de julio de 2003*, México, IEDF, 2003.

_____, *Memoria del Plebiscito 2002*, México, IEDF, 2002.

_____, *Memoria General del Proceso Electoral 2000*, México, IEDF, 2000.

_____, *Memoria General del Proceso Electoral 2003*, México, IEDF, 2003.

_____, *URNA*, Carta Informativa del Instituto Electoral del Distrito Federal, año 4, núm. 23, mayo, México, IEDF, 2003.

_____, *URNA*, Carta Informativa del Instituto Electoral del Distrito Federal, año 4, núm. 24, junio, México, IEDF, 2003.

_____, *URNA*, Carta Informativa del Instituto Electoral del Distrito Federal, año 5, núm. 28, marzo, México, IEDF, 2004.

_____, *URNA*, Carta Informativa del Instituto Electoral del Distrito Federal, año 5, núm. 29, mayo, México, IEDF, 2004.

Confiabilidad y auditabilidad de las urnas electrónicas

AUDITABILIDAD DE URNAS ELECTRÓNICAS

Silvia Beatriz González Brambila,
Universidad Autónoma Metropolitana (UAM)

Doctora en Ciencias de la Computación, coordinadora de la Licenciatura de Ingeniería en Computación de la UAM, unidad Azcapotzalco. Área de Investigación: Razonamiento Cualitativo.

Francisco Javier Zaragoza Martínez
UAM

Doctor en Combinatoria y Optimización, profesor - investigador titular del Departamento de Sistemas de la UAM, unidad Azcapotzalco. Área de investigación: Optimización Combinatoria.

Josué Figueroa González
UAM

Ingeniero en Electrónica, cursa la Maestría en Ciencias de la Computación en la UAM, unidad Azcapotzalco. Área de investigación: Sistemas Digitales (licenciatura), Cómputo Científico y Organización de Sistemas (maestría).

RESUMEN

El objetivo del documento es analizar el concepto y propósito de la auditabilidad en urnas electrónicas, se describe un panorama general sobre la auditabilidad de los sistemas convencionales y de los sistemas de votación en los que intervienen las urnas electrónicas. Se revisa el diseño de un sistema que permite una auditoría sencilla, analizando las vulnerabilidades de estos sistemas desde un punto de vista de auditabilidad y no de seguridad, se ofrecen algunas propuestas de solución a los problemas de vulnerabilidad.

INTRODUCCIÓN

En esta ponencia se analizará el concepto de auditabilidad, su propósito y todos los conceptos que involucra un sistema de votación no basado

en boletas, en este caso, el de una urna electrónica. Se revisarán los conceptos que se relacionan con la auditabilidad; se estudiarán las etapas que forman el sistema de votación en urnas electrónicas, así como los documentos que serán de utilidad en caso de una auditoría, se revisará el proceso de diseño de un sistema que garantice un proceso de auditoría sencillo y eficiente.

Lo primero que se debe conocer es la forma en que está constituido el sistema de votación en una urna electrónica, este sistema lo podemos ver como la unión de tres etapas: pre votación, votación, post votación.

La etapa de pre votación se forma por los pasos que se efectúan para cargar aplicaciones y archivos de configuración en la urna electrónica. En la etapa de votación los electores realizan el proceso de votación, esta etapa es la encargada de ir almacenando los votos. La etapa de post votación tiene como objetivo efectuar el conteo de los votos y generar las actas de resultados. Cabe señalar que aunque esta ponencia revisa el concepto de auditabilidad en las tres etapas, se enfoca en la etapa de votación.

A continuación se presentan algunas definiciones básicas que se consideran de utilidad para comprender los conceptos que se irán revisando más adelante.

1. Definiciones Básicas

Las definiciones básicas que se pueden encontrar en un proceso de auditoría a un sistema cuyo funcionamiento está basado en el conteo, específicamente en el de una urna electrónica, son las siguientes: auditoría, auditabilidad, confianza del votante y confianza del público en general.[75]

1.1 Auditoría

Realizar una auditoría de un sistema basado en el conteo es examinar el sistema para determinar si los resultados que este sistema reporta son

[75] Auditability and Voter-Confidence in Direct-Recording (DRE) Voting Systems, http://www.constitutionproject.org/eri/auditability1.pdf

adecuados de acuerdo a la entrada y a las acciones del proceso. Uno de estos sistemas de conteo es el que nos ocupa la urna electrónica. Una auditoría en este caso, servirá para corroborar que el total de votos que registró la urna es congruente con el total de votos que recibieron en conjunto los candidatos participantes en la elección y con el total de votos que emitieron los votantes.

1.2 Auditabilidad

Es determinar cuáles de los datos en los que se basará la auditoría están disponibles para ser usados y poder obtener un reporte adecuado. Se presenta un problema en la auditabilidad cuando los datos no se encuentran disponibles o el obtenerlos resulta muy difícil o costoso.

1.3 Confianza del votante

Se refiere a la certeza que tiene un votante de que su elección ha sido bien interpretada por la computadora. Además el votante quiere estar seguro de que su voto ha sido sumado correctamente a los votos que emitieron los demás ciudadanos.

1.4 Confianza del público en general

Esto es el nivel de aceptación que tiene el público en general, tomando como un hecho, que los resultados representan las verdaderas elecciones de los votantes. Este nivel de confianza incluye la suma de las confianzas de los votantes, además de otros factores como el desempeño de los programas computacionales, los resultados de una auditoría y los reportes de la elección. Una vez que se han revisado las definiciones básicas, se estudiará cuál es el propósito de realizar una auditoría a este tipo de sistemas.

2. Propósitos de una auditoría

Una auditoría tiene al menos dos propósitos, el primero es determinar si la ley y los reglamentos se siguieron en el proceso de votación, y proporcionar evidencia de los errores que pudieron haber ocurrido, ya sea de manera accidental o de manera deliberada; el segundo es el de contribuir

al aumento de confianza en las instituciones en caso de que la auditoría demuestre que los resultados son correctos.

3. Auditorías en los sistemas de elección convencionales

El sistema de elecciones actuales en México (basado en boletas) también se somete a un proceso de auditabilidad. Este proceso puede parecer más sencillo que el de una urna electrónica, pero antes de estudiar la auditabilidad se revisará el funcionamiento básico del proceso de votación en estos sistemas.

- El votante recibe una boleta donde se encuentran los partidos políticos y candidatos que contienden para cierta elección.
- El votante marca el símbolo del partido y lo deposita en una urna.
- Una vez que se ha terminado la jornada electoral, se extraen las boletas marcadas de las urnas para llevar a cabo el conteo de los votos que obtuvo cada partido político, reportando los resultados en las actas de escrutinio. Estas actas y las boletas marcadas proporcionan una herramienta fundamental para el proceso de auditoría, la forma más común y sencilla, aunque tal vez no la más conveniente, es contar manualmente todas las boletas para verificar que los resultados que se reportaron en las actas concuerdan con las boletas.

En caso de que se realice de manera adecuada, los resultados que arroje la auditoría deberán ser iguales a los de la votación.

4. Sistemas de almacenamiento directo del voto

Los sistemas de almacenamiento directo del voto, llamados DRE (por sus siglas en inglés: *Direct-Recording Voting Systems*), son aquellos que ya no utilizan las boletas tradicionales. Aunque existen varios tipos, podemos mencionar tres: los de botones, los mini interruptores y los que utilizan una pantalla táctil como interfaz.

Los de botones reemplazaron al sistema de palancas que se empleaba en Estados Unidos, y consisten en presionar los botones que contienen los logotipos de los partidos políticos o nombres de los candidatos para

emitir el voto. Los que utilizan mini interruptores son sistemas que se activan mediante el toque de los votantes sobre una superficie flexible que se coloca encima de otra en donde se muestran las opciones disponibles para elegir. Un sistema más novedoso involucra el despliegue del logotipo de los partidos políticos y el nombre de los candidatos en un monitor con áreas sensibles al tacto; al presionar el área donde se encuentra el nombre de un candidato o el logotipo de un partido político, el sistema responde de acuerdo a la programación. Antes de analizar estos sistemas, es necesario considerar que el voto es un sistema complejo en el que intervienen personas, procedimientos, dispositivos y máquinas, y actividades, y no todo depende del desarrollo adecuado del *software* de votación. De aquí, que los tres criterios que debemos tener en cuenta al momento de diseñar sistemas de votación son los siguientes:

- Que sea sencillo para el votante emitir su voto
- Que procese correctamente la opción elegida
- Que obtenga la confianza del público en los resultados que arroje el sistema

4.1 Diseño

El diseño de estos sistemas debe asegurar la confianza del votante y proporcionar los medios para una revisión eficiente por parte de un auditor.

Estos sistemas de votación están formados por tres unidades:

- Entrada del voto
- Totalización del voto
- Almacenamiento del voto

4.1.1 Unidad de entrada del voto

La entrada de esta sección es la elección del votante, y su salida es la elección final del votante, considerando que se tiene una etapa en donde el votante puede corregir su voto antes de confirmar; una vez que el votante concluyó el proceso de selección, no se permitirá, gracias a la lógica del sistema, que el votante pueda realizar selecciones adicionales.

Para esta unidad se deben considerar tres aspectos técnicos muy importantes:

- El que los votos se almacenen en localidades de memoria elegidas de manera aleatoria conforme se generen, de manera que no se pueda tener una relación de votante – voto de acuerdo al orden en que los votos se vayan almacenando.
- Que una vez que el voto ha sido almacenado, debe convertirse en un sistema de "solo lectura", para evitar que pueda ser modificado.
- Ir almacenando las sumas parciales de los votos que, como medida de seguridad, deberán ir cifrados.

Es conveniente que los votos o el archivo con la suma parcial de los votos se almacenen de manera aleatoria, aunque realmente es de una forma pseudo aleatoria.[76]

4.1.2 Unidad de totalización del voto

La función de esta unidad es realizar la suma de los votos individuales tal y como se obtienen y, al finalizar la jornada electoral, reportar el total de votos que obtuvo cada candidato o partido político, al igual que registrar el número de votos nulos obtenidos de los votantes que decidieron no elegir ningún candidato. Una vez que se tienen los resultados de los votos obtenidos por los diferentes partidos políticos y los votos nulos, el total de esta suma debe ser igual al total de votantes que utilizaron el sistema.

4.1.3 Unidad de almacenamiento del voto

Almacenar los resultados es de gran importancia en caso de que se necesite un recuento. Por ello es necesario que las tres secciones funcionen adecuadamente y que sean sometidas a varias pruebas antes de la elección, por ejemplo: si la sección encargada de registrar el voto no funciona

[76] Niels Ferguson y Bruce Schneier, *Practical cryptography*, Editorial Wiley, 2003.

adecuadamente, ya sea por fallas accidentales o no, los resultados obtenidos no coincidirán con las elecciones de los votantes, y ello generará una mayor desconfianza. Estos resultados tendrán que almacenarse en varios medios físicos y deberán poder ser examinados en cualquier otra máquina, igual que el almacenamiento en la memoria, aquí los datos también deben encriptarse.

5. Vulnerabilidad

La vulnerabilidad de un sistema de almacenamiento directo del voto en esta ponencia, no se refiere a las partes de ese sistema que pudieran ser alteradas, sino a la desconfianza que se puede generar debido a su uso. A través de la evolución de los sistemas de votación que no utilizan boletas, han surgido varias preguntas, tal vez la más común es: ¿Existen métodos que hagan posible el manipular una elección utilizando computadoras?[77]

R. Saltman,[78] consultor en políticas electorales y tecnología, señala lo siguiente: La administración de un sistema consiste en cuatro elementos: personas, procedimientos establecidos, dispositivos y máquinas, y finalmente actividades. La administración del sistema debe ser llevada a cabo, de acuerdo con los procedimientos establecidos por el personal que utiliza las máquinas o dispositivos. Ahora, con el uso de computadoras, el nivel de desconfianza aumenta debido a la posibilidad de que el funcionamiento de estos sistemas sea incorrecto debido a los elementos mencionados. Por eso, en lugar de explicar las formas en que se podría utilizar una computadora para manipular o alterar las elecciones, se tienen que estudiar los procedimientos que utilizarán los responsables de la elección para asegurar que los resultados reflejan de forma correcta las elecciones de los votantes.

Los procedimientos a seguir son *a)* adquirir *software* y *hardware* de acuerdo a las especificaciones que se deban cumplir para la elaboración

[77] Auditability of non-ballot, poll-site voting systems, http://vote.nist.gov/pospapers/Saltman-AuditabilityofDREs(Revised)2003.pdf*

[78] *Op. cit.*

del sistema, *b)* verificar la integridad y confiabilidad del *software* y del *hardware*, *c)* proteger el *software* y el *hardware* contra accesos no autorizados y *d)* empleo eficiente del *hardware* y del *software* en las operaciones de la elección. Ahora analizaremos las diferentes vulnerabilidades desde el punto de vista de la auditabilidad que pueden presentarse en los distintos tipos de sistemas de votación.

5.1 Vulnerabilidad de los sistemas de elección convencionales

Estos sistemas no son necesariamente menos vulnerables a los errores o fraudes de los sistemas que no utilizan boletas. Dos de sus principales vulnerabilidades son:

- Los que leerán las boletas pueden cometer errores, sobre todo cuando las marcas en las boletas no son lo bastante claras, como puede ser el caso de que al marcar un partido político se alcance a marcar otro, y quede al criterio del encargado (escrutador) decidir a qué partido se le otorga el voto.
- Al momento en que se cuentan los votos, se pueden producir errores ya sea por equivocación o de forma deliberada, sobre todo si se cuenta una gran cantidad de boletas.

5.2 Vulnerabilidad en los sistemas de almacenamiento directo del voto

La principal vulnerabilidad de este tipo de sistemas es que no tienen un comprobante que sirva para que el votante sienta que su voto fue registrado y contabilizado de manera adecuada. Incluso si se imprime un comprobante, éste sigue dependiendo del programa que se encuentra dentro de la computadora.

"El hecho de que un votante pueda ver sus opciones en una pantalla, o que reciba un comprobante impreso de su elección, no garantiza que esas elecciones fueron almacenadas en la máquina y contabilizadas para generar los resultados de la elección".[79]

[79] *Op. cit.*

Este aspecto es del que más desconfían los votantes, y esa desconfianza de la ciudadanía hacia las máquinas y, por ende, hacia las instituciones. Ahora se examinarán algunas de las propuestas de diseño de los sistemas que permitirán resolver este aspecto.

6. Solución al problema de auditabilidad en los sistemas de almacenamiento directo del voto

Una solución que se ha propuesto en los distintos países con mayor experiencia en el voto electrónico, como es el caso de Estados Unidos, es que se genere una especie de boleta con el voto registrado, y que ésta se introduzca posteriormente en un depósito encargado de contar los votos. Así el votante tendría mayor confianza en que su voto ha sido contabilizado, pero esto implica la desventaja de que además de no ser estrictamente un sistema de voto directo, debido a que no elimina el uso de boletas, necesita más dispositivos de impresión, lo que aumenta el tiempo invertido en cada voto y siempre existe la posibilidad de que el votante no deposite la segunda boleta en la urna correspondiente.[80]

6.1 Recomendaciones

Existen varias recomendaciones que se deben tomar en cuenta al momento de diseñar el sistema, éstas se hacen tratando de que el sistema dependa lo menos posible de los factores humanos que intervienen en el momento de la votación, y con la intención de generar un mayor nivel de confianza del votante y, posteriormente, del público en general.[81]

a. Inhabilitación del equipo después de que se ha concluido el proceso de votación

Cada vez que un elector concluya de emitir su voto, el equipo se deshabilitará y no podrá recibir otro voto hasta que se habilite nuevamente por alguno de los responsables del proceso de votación.

[80] Auditability and Voter-Confidence in Direct-Recording (DRE) Voting Systems, http://www.constitutionproject.org/eri/auditability1.pdf

[81] Auditability of non-ballot, poll-site voting systems, http://vote.nist.gov/pospapers/Saltman-AuditabilityofDREs(Revised)2003.pdf*

b. Reporte directo hacia el votante de la contribución de su voto

Una prueba que ha demostrado generar un mayor nivel de confianza es un pequeño contador visible para los votantes, que se incrementa en uno después de que se ha votado, aunque no refleja que el voto se le otorgó al candidato de su elección, aún así el hecho de que el número de votos se incremente en uno, produce un aumento en el nivel de confianza.

c. Almacenar los votos y contabilizarlos en otra máquina

Es importante que los votos se almacenen en algún medio físico que pueda insertarse en otro dispositivo además de que se almacenen en la memoria interna de la urna que servirá como respaldo de los resultados.

d. Suma de los votos y de los votos nulos

Una buena prueba para una auditoría, es la suma de los votos, de los votos que registró cada candidato y de los votos nulos, estos pueden manejarse por separado y después sumarse, o ir incrementándose con algún contador cada que se vote, independientemente de a qué candidato se le otorgó el voto.

e. Asegurar que todos los tipos de elecciones se le presenten al votante

Puede utilizarse un indicador que le avise al votante si le falta votar en alguna de las elecciones o el sistema puede presentar todas las votaciones en orden secuencial.

f. Facilidad de pruebas

El sistema debe ser fácil de probar por parte de las autoridades encargadas de los procesos de votación. Estas pruebas deben realizarse en presencia de los candidatos o representantes de partidos interesados, y no deberán afectar el futuro desempeño de la urna electrónica.

Otros tipos de auditabilidad son las relacionadas con el *software* y el *hardware* que se emplearán en el sistema. Todo el *software* y el *hardware* que se utilizará debe verificarse siguiendo varios procedimientos. Como

la integridad de las votaciones depende del *software* y del *hardware*, se tienen que realizar pruebas.

El *software* debe ser escrito para que sea sencillo de modificar de acuerdo al tipo de elección, se deben tener sólo espacios en blanco para insertar los datos de partidos políticos, candidatos, y tipo de elección, sin tener que modificar ninguna de las rutinas de registro de votos, de totalización, o de almacenamiento. Se tienen que realizar pruebas en el *software* para descubrir si existen rutinas ocultas que puedan modificarse antes de cargar las aplicaciones en los dispositivos, esto justamente se logra con un código fuente detallado, donde se explique claramente la función de cada módulo, las entradas que recibe y las salidas que produce, y realizar las pruebas que menciona la recomendación f. Se tiene que hacer reportes de la forma en que el *software* se instaló en los equipos, la manera en que se configuró, incluso en la forma en que se almacenaron y distribuyeron los equipos antes del proceso electoral, esto evitará los rumores de modificación del programa.

7. Aplicando los conceptos al desarrollo de una urna electrónica

Ahora que se han revisado los conceptos y aspectos relacionados con la auditabilidad de los sistemas de voto directo, se procederá a aplicar lo estudiado en el desarrollo de una urna electrónica.

7.1 Subsistemas de la urna electrónica

Como se mencionó en la introducción, la jornada electoral se divide en tres etapas: pre votación, votación y post votación.

7.2 Auditabilidad de la etapa de pre votación

La etapa de pre votación incluye todos los procedimientos y configuración que se realizarán antes de que la urna electrónica entre en funcionamiento.

En esta etapa, lo que se desea auditar es lo siguiente:

- *Hardware*
- Código fuente de las aplicaciones
- Configuración y carga de información en la urna electrónica

El *hardware* debe contar con todas sus especificaciones, y haber acreditado las pruebas que se le apliquen para verificar que es adecuado para la función que será utilizado, como la duración de la batería, resistencia a las condiciones climáticas y al trato físico y funcionamiento de componentes internos; para el sistema que se desarrolla se tendrá un reporte del funcionamiento de los componentes. El *software*, que incluye el código fuente, el sistema operativo y los archivos de configuración, tiene que realizarse de la manera más sencilla posible, siempre con indicaciones claras que permitan a los interesados llevarle a cabo auditorías, que básicamente consistirían en revisarlo, como se explicó antes, la modificación de este código para futuras elecciones debe consistir en sólo cambiar imágenes, nombres o logotipos de los partidos políticos.

Algo importante es el uso de *software* de código libre, lo que permitirá que cualquier persona tenga acceso a él, pero esto toma una mayor importancia al momento de elegir el sistema operativo, el cual debe ser de acceso libre para poder utilizarlo por completo o sólo partes de él sin necesidad de preocuparse por cuestiones de licencias.

Tratar de entender y analizar un programa completo es una tarea laboriosa y difícil que requiere de experiencia. Aunque no existen herramientas disponibles que permitan automatizar por completo este proceso, sí hay herramientas que hacen posible auditar el código fuente a través de búsquedas de las llamadas a las funciones y que revisan algunas cuestiones de seguridad en la implementación, tales como: sobre flujo, inicialización de variables, manejo de archivos.

Entre las herramientas de este tipo, están RATS (*Rouge Auditing Tool for Security*), Flawfinder e ITS4 (*It's The Software, Stupid![Security Scanner]*).

La configuración de las urnas debe hacerse en presencia de los interesados, es decir, de los representantes de partidos políticos, candidatos, instituciones electorales y observadores autorizados para las elecciones y se obtendrá un reporte para conocimiento y aceptación de los mismos.

Antes de la etapa de votación, se obtiene una de las primeras pruebas de auditoría que es el acta inicial, la cual debe contener los datos de la casilla específica. Al ser el acta inicial, el número de votos de los partidos contendientes y de los votos nulos deberá estar en cero; esta acta

será firmada por los representantes de los partidos políticos en señal de acuerdo.

7.3 Auditabilidad de la etapa de votación

La etapa de votación se divide en tres unidades: entrada del voto, totalización y almacenamiento. Ahora se revisarán los aspectos auditables en cada una.

En la entrada del voto, que inicia cuando se elige una opción y termina cuando se ha confirmado totalmente la elección, se obtiene un comprobante impreso que aunque no se le entregará al votante, sirve para que éste tenga más confianza de que su voto se contabilizó correctamente, lo que cumple en parte la recomendación b. Una de las recomendaciones que cumple este sistema es la parte de inhabilitación del sistema una vez que un votante ha concluido su participación (recomendación a).

Otra de las pruebas más importantes para una posterior auditoría es un archivo de eventos o bitácora, la cual irá registrando todos los eventos que ocurran en el proceso de votación: la hora en que se habilitó la urna, el funcionamiento de los componentes, los distintos errores que pudieran ocurrir debido a componentes físicos, si se intentó y si se logró o no modificar el archivo que almacena los resultados, la aplicación o el contenido de los dispositivos físicos que almacenan los votos, además de la hora en que se inhabilitó la urna.

Para la elaboración de esta bitácora se tienen las siguientes opciones: La construcción de este archivo va desde lo más simple hasta métodos complejos que permiten examinar detalladamente un sistema. Se puede añadir en el archivo fechas, horas, y reportes de los eventos que se presenten durante el proceso de la votación. Un enfoque más detallado de esta bitácora consistirá en obtener información detallada de todas las actividades que se ejecutaron en la urna, además de las mencionadas anteriormente, y se debe verificar a fondo las características del *hardware*, la forma en que está instalado y la manera en que el sistema operativo lo reconoce.[82]

[82] Keith K. Seglem, *Handbook of computer crime investigation*, Editorial Academic Press, 2002.

Uno más de los aspectos importantes en la auditabilidad es el poder obtener información de los archivos en caso de que éstos hayan sido modificados, y registrarlo en el archivo de bitácora. También es necesario registrar las características de los archivos de configuración, de las aplicaciones y de almacenamiento de los votos, dichas características incluyen la fecha de creación, de modificación, los permisos que se tienen y si se intentó o logró modificar alguno de los archivos. Aunque la sección de totalización entra en esta etapa, el elemento auditable que proporciona aparece hasta la etapa de post votación, es decir, en el acta final de votación; pero aquí podemos tener un indicador que se incremente cada que se realizó un voto, independientemente de a qué partido político se le otorgó el voto o si fue un voto nulo, y el presentarle al votante un indicador de que su voto se contabilizó aumenta el nivel de confianza. Finalmente en la sección de almacenamiento, y de acuerdo a lo establecido en la recomendación c, se almacenarán los votos tanto en la memoria interna de la urna como en dos dispositivos extraíbles, lo que permitirá poder contabilizar los votos en otro dispositivo.

7.4 Auditabilidad de la etapa de post votación

En la etapa de post votación se tendrán las actas finales que deberán indicar la hora de cierre, datos de la casilla, el número de votos que obtuvo cada partido político y el número de votos nulos, y el total de votantes que participaron en la elección. Es aquí en donde entra la recomendación d, la suma de los votos de cada partido político más la suma de los votos nulos, deberá ser igual al número de votantes que utilizaron la urna. Pero además, al tener los comprobantes impresos, cuya suma en general deberá ser igual al total de votantes y la suma de votos de los comprobantes para cada partido en particular, al igual que la suma de los votos nulos deberá coincidir con lo especificado en las actas finales.

Este proyecto incluye otras dos etapas que se refieren a la transmisión de la información, aquí se generarán reportes que indicarán si la comunicación entre los equipos ha sido exitosa o si alguien trató de interrumpirla.

[83] *Op. cit.*

En este caso el archivo de reporte también incluirá datos sencillos de obtener como el que la comunicación y transmisión fue exitosa, pero al igual que el archivo de bitácora, puede elaborarse con datos más detallados.[83]

Otra manera de auditoría para el votante que se emplea después de que ha terminado el proceso de votación, es el que tenga un número o clave, por ejemplo, su clave única de registro de población (CURP) y elaborar una página en Internet en la cual al escribir esa clave aparezca un mensaje que indique si fue contabilizado su voto o no, así el votante tiene tres elementos para la auditabilidad:

- El comprobante impreso del voto.
- El ver que el contador de votos se incrementa en uno después de que terminó su elección.
- El poder verificar, a través de su clave, si su voto se contabilizó.

8. Conclusiones

La auditabilidad se refiere a la obtención de documentos o datos que nos servirán en caso de que se quiera o requiera hacer una auditoría a un sistema. Los procesos de auditoría se utilizan fundamentalmente para generar la confianza de los votantes y del público en general hacia las instituciones.

La auditoría de estos sistemas no debe basarse en el recuento de votos, sino en el estudio detallado y en la verificación de la integridad del código fuente y de los componentes físicos, y debe estar respaldada en una serie de pruebas que garanticen el correcto funcionamiento de la urna electrónica.

Para llevar a cabo una auditoría a un alto nivel es necesario que el sistema haya sido desarrollado con el fin de garantizar el correcto funcionamiento del *software* y del *hardware*.

Finalmente, el proceso de votación depende de personas, instituciones y de dispositivos, la confianza que se tendrá en los dispositivos es sólo de funcionamiento, mientras que la mayor responsabilidad de generar un alto nivel de confianza en este tipo de procesos recaerá en las instituciones y en el personal responsable.

BIBLIOGRAFÍA

SEGLEM, Keith K, *Handbook of computer crime investigation*, Academic Press, 2002.

FERGUSON, Niels y Bruce Schneier, *Practical cryptography*, Wiley, 2003.

Páginas de Internet

Auditability and Voter-Confidence in Direct-Recording (DRE) Voting Systems, http://www.constitutionproject.org/eri/auditability1.pdf

Auditability of non-ballot, poll-site voting systems, http://vote.nist.gov/pospapers/Saltman-AuditabilityofDREs(Revised)2003.pdf*

PERCEPCIÓN Y REACCIÓN ANTE LAS URNAS ELECTRÓNICAS

Silvia González Brambila
Universidad Autónoma Metropolitana (UAM)
Doctora en Ciencias de la Computación y coordinadora de la Licenciatura de Ingeniería en Computación de la UAM, unidad Azcapotzalco.

Georgina Pulido Rodríguez
UAM
Maestra en Ciencias de la Computación, y profesora de la División de Ciencias Básicas e Ingeniería de la UAM.

Yadira Zavala Osorio
UAM
Maestra en Ingeniería con especialidad en Planeación y profesora de la División de Ciencias Básicas e Ingeniería de la UAM.

Eugenia Reyes Morán
UAM
Cursa la Licenciatura de Ingeniería en Computación en la UAM.

Rodrigo A. Castro Campos
UAM
Cursa la Licenciatura de Ingeniería en Computación en la UAM.

Ariana Cruz Trejo
UAM
Cursa la Licenciatura de Ingeniería en Computación en la UAM.

RESUMEN

A través de una muestra semi-aleatoria se levantó una encuesta que permite sondear cuál sería la disposición que tendría la población del Distrito Federal para utilizar urnas electrónicas en una elección y cuál sería su grado de confianza en los resultados que de ella se deriven. Se obtuvo un intervalo de confianza de 95% para la proporción de personas que no

usarían la urna electrónica y otro para la proporción de personas que no confiaría en la elección.

INTRODUCCIÓN

Por medio del voto no sólo se elige libremente y en secreto a las autoridades que nos gobiernan, sino además, con esta forma de expresión, se participa en la consolidación de la democracia.

El derecho al voto ha tenido diversos procesos en la historia de nuestro país:

En la *Constitución Política de los Estados Unidos Mexicanos* de 1917 se declaró que el voto es universal, libre, directo y secreto para los cargos de elección popular, y que los partidos políticos son entidades de interés público.

En 1935, sectores significativos de mujeres organizadas se coordinaron en el Frente Único Pro Derechos de la Mujer (FUPDM) para exigir el sufragio. Los legisladores reformaron la Constitución y en 1953 las mujeres mexicanas ejercieron por primera vez su derecho al voto.

Las sucesivas reformas electorales de 1977, 1986, 1989, 1990, 1993, 1994, y 1996 estuvieron destinadas a garantizar elecciones plenamente legales, limpias, imparciales y respetuosas de la voluntad popular.

En 1997, por primera vez en la historia de México, los resultados preliminares de las votaciones para elecciones federales de todo el país se dieron a conocer públicamente, casilla por casilla, a través de Internet, durante la noche de la jornada electoral y en la mañana del día siguiente. Así, la utilización de nuevos mecanismos tecnológicos en el marco de los procesos electorales cobró gran trascendencia y se comenzó a vislumbrar la aplicación de otro tipo de tecnología para hacer más eficiente el desarrollo de las etapas de dichos procesos.

Han sido tiempos de modernización en el ámbito electoral, y hoy es claro que cualquier sistema de votación, tradicional o innovador, debe permitir que todos los ciudadanos manifiesten plenamente su derecho al voto, sin importar el grado de analfabetismo y/o discapacidad física.

En la actualidad, entre las modificaciones que se plantean está utilizar urnas electrónicas en los procesos de elección. Algunos estados de la

república han efectuado pruebas piloto para determinar su confiabilidad de uso, además de la facilidad para realizar la votación.

En América Latina uno de los países que ha utilizado urnas electrónicas en sus elecciones es Brasil, donde a pesar de que los ciudadanos tuvieron que apretar hasta 25 teclas para dar un voto a su candidato, el uso de las urnas electrónicas permitió conocer el resultado definitivo sólo tres horas después del cierre de los colegios electorales.

Otros países que han implantado el voto electrónico son:

- Estados Unidos
- Bélgica
- Filipinas
- India
- Francia
- España
- Argentina
- Venezuela
- Japón.

1. La encuesta

A continuación se presenta la encuesta que se realizó para conocer el grado de aceptación y confiabilidad en el uso de la urna electrónica en los procesos electorales así como de sus resultados.

La encuesta tuvo el diseño que se muestra en la figura 1.

Figura1.

Encuesta

Datos generales

¿En qué delegación vive?

Álvaro Obregón		1
Azcapotzalco		2
Benito Juárez		3
Coyoacán		4
Cuajimalpa de Morelos		5

Cuauhtémoc		6
Gustavo A. Madero		7
Iztacalco		8
Iztapalapa		9
Magdalena Contreras, La		10

Miguel Hidalgo		11
Milpa Alta		12
Tláhuac		13
Tlalpan		14
Venustiano Carranza		15
Xochimilco		16

¿Cuál es su escolaridad?

Primaria	
Secundaria	
Preparatoria/bachillerato	
Licenciatura	
Posgrado	

¿Rango de edad?

De 18 a 20	
De 21 a 30	
De 31 a 40	
De 41 a 50	
De 51 a 60	
Más de 60	

¿Cómo se define a usted mismo?

Trabajador por cuenta propia	
Empleado	
Jubilado / pensionado	
Ama de casa	
Estudiante	
Desempleado	

PREGUNTAS

¿Qué tan frecuentemente usa usted los cajeros automáticos?

Al menos dos veces al mes	
Una vez al mes	
Casi nunca	
Nunca	

¿Cómo utiliza usted un teléfono celular?

Envía mensajes y habla	
Solamente habla	
Los ha utilizado pocas veces	
Nunca	

¿Utiliza usted computadora en su trabajo o en su casa?

Me es indispensable	
Casi siempre	
Ocasionalmente	
Nunca	

Calculadoras, ¿las usa usted?

Siempre	
Casi siempre	
De vez en cuando	
Nunca	

El horno de microondas, ¿usted lo emplea?

Siempre	
Casi siempre	
De vez en cuando	

URNA ELECTRÓNICA

¿Está usted dispuesto a utilizarla?

Sí	Sólo si me capacitan	No estoy seguro	No
○	○	○	○

Si se votara a través de una urna electrónica ¿confiaría usted en los resultados?

Sí	Sí con condiciones	No estoy seguro	No
○	○	○	○

¿Tiene usted algún comentario?

_____

_____

_____

_____

Dicha encuesta se aplicó a 536 personas en supermercados y tianguis de las delegaciones Azcapotzalco, Iztapalapa, Cuauhtémoc y Gustavo A. Madero. El número de encuestados conforme a la delegación de procedencia se presenta en la tabla 1.

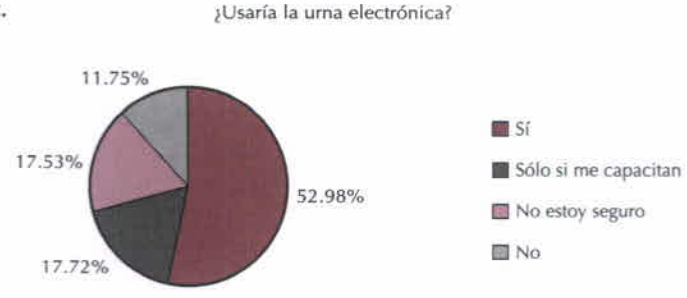
Tabla 1.

Delegación	Personas encuestadas
Azcapotzalco	151
Iztapalapa	116
Gustavo A. Madero	45
Coyoacán	33
Iztacalco	33
Cuauhtémoc	31
Álvaro Obregón	27
Miguel Hidalgo	26
Benito Juárez	23
Tlalpan	16
Magdalena Contreras, La	9
Cuajimalpa de Morelos	7
Venustiano Carranza	6
Xochimilco	6
Tláhuac	4
Milpa Alta	2

2. Estudio estadístico

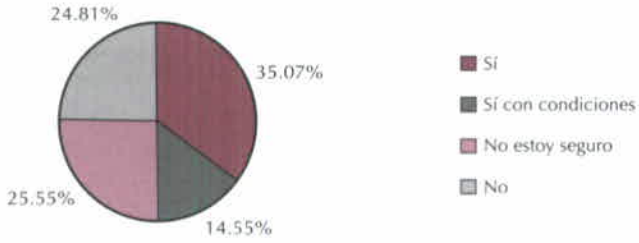
De acuerdo con los datos de la muestra, alrededor de 12% de los encuestados contestó que no usaría la urna electrónica (véase figura 2).

Figura 2.



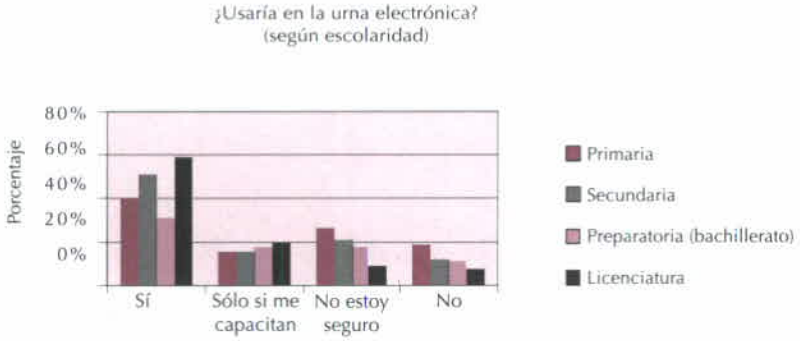
Cerca de 25% de los encuestados manifestó que no confiaría en los resultados que se obtuvieran de una urna electrónica, como así puede verse en la figura 3.

Figura 3.



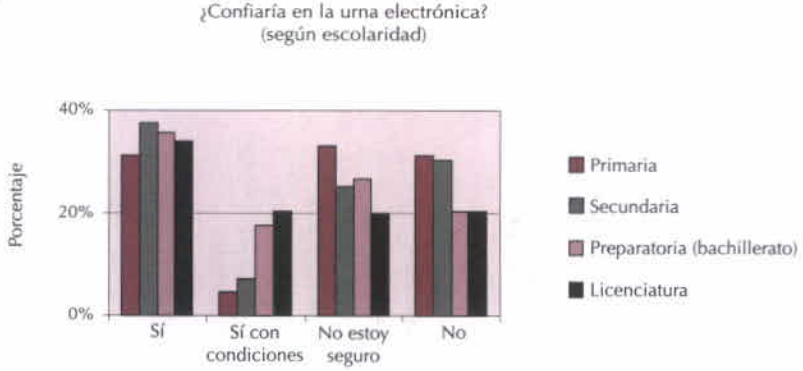
El grado de escolaridad de una persona no determina si está dispuesta o no a utilizar una urna electrónica, como puede observarse en la figura 4.

Figura 4.



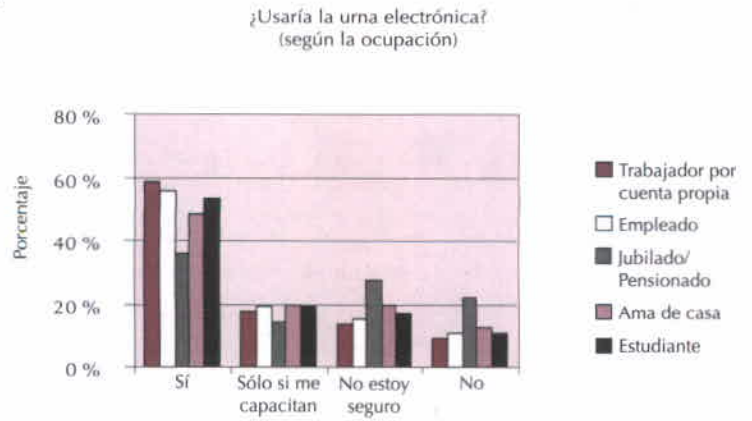
En la figura 5 se aprecia que un porcentaje alto de la población encuestada requiere de campañas informativas que le permitan incrementar su grado de confianza en los resultados que se obtendrían a través del uso de la urna electrónica.

Figura 5.



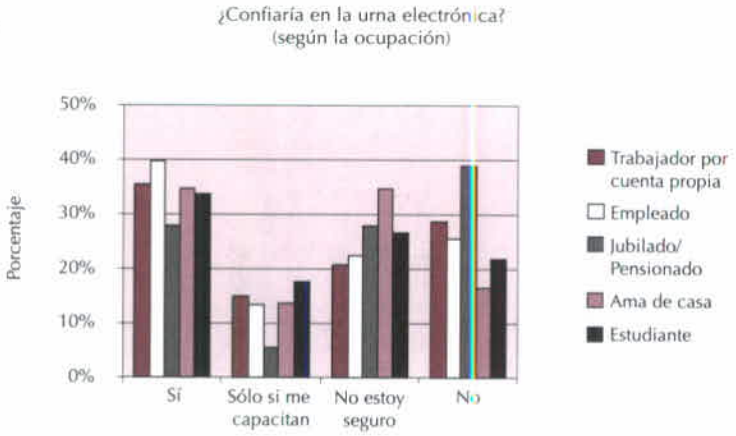
Casi la mitad de los entrevistados está dispuesta a utilizar la urna electrónica incondicional e independientemente de su ocupación. Véase figura 6.

Figura 6.



Aproximadamente 30% de la población encuestada requiere de campañas informativas que le permitan generar confianza respecto de la utilización de la urna electrónica (véase figura 7).

Figura 7.



2. Cálculo del intervalo de confianza para el número de personas encuestadas que harían uso de la urna electrónica

Para este cálculo, se consideró el número de elementos de la muestra, 536. Del total de encuestados, 62 indicaron que no usarían la urna electrónica. El intervalo de 95% de confianza se calcula de acuerdo con la expresión:

$$\left(\hat{p} - z\sqrt{\frac{\hat{p}(1-\hat{p})}{n}}, \hat{p} + z\sqrt{\frac{\hat{p}(1-\hat{p})}{n}}\right)$$

Donde z es el valor de la distribución normal estándar que corresponde a 95% en área central y es la proporción muestral.

El valor de la proporción muestral que señaló *no usaría la urna electrónica* es de 62/536. Al reemplazar estos valores se obtiene el intervalo (0.11, 0.12).

En el caso de la respuesta *no confiaría en los resultados*, la proporción muestral fue de 133/536. El intervalo de confianza calculado es (0.212, 0.265).

3. Conclusiones

Es importante que el diseño de una urna electrónica considere las características del voto como son: universal, libre, directo y secreto. E incluya

aquellos procedimientos que permitan a las personas con capacidades diferentes manifestar su elección.

Entre las ventajas que se tendrían al implantar el uso de la urna electrónica en el Distrito Federal se encuentran las siguientes:

- Menor costo, al usar tecnología que puede emplearse en muchas elecciones ya que lo único que debe modificarse son los datos de la o las elecciones específicas a realizarse. Actualmente se requiere la impresión de boletas con diferentes sistemas de seguridad (como papel seguridad, bandas de seguridad, marcas de agua) que elevan los costos.
- Menor tiempo para obtener resultados, ya que los votos se almacenan de forma digital y la totalización no requiere del conteo manual que actualmente se efectúa.
- Aumento en la confiabilidad de resultados, esto se logra gracias a los diferentes sistemas de auditoría que pueden estar involucrados en las diferentes etapas del proceso de votación.
- Disminución de errores; actualmente durante el conteo manual los funcionarios de casilla interpretan los votos, lo cual conlleva a obtener votos nulos, y esto puede eliminarse en el voto electrónico, ya que el usuario puede manifestar de forma más automática su elección por algún candidato o su abstención.
- Disminución en el número de fraudes, al utilizar una nueva tecnología las personas que de forma deliberada cometen delitos deberán adquirir los conocimientos para poder efectuarlos. Si bien es cierto que ninguna tecnología en ningún sistema podría garantizar la seguridad total, pueden diseñarse urnas electrónicas que permitan considerarse seguras dentro de los siguientes 5 o 10 años.

Las principales desventajas de cualquier sistema de votación electrónica son la capacitación, el miedo y la desconfianza hacia la tecnología de parte de ciertos sectores de la población.

A pesar de que no se ha ofrecido información acerca de los beneficios de las urna electrónica en el Distrito Federal se observa una gran disposición al uso de la misma, así como de confianza en los resultados.

De los resultados obtenidos puede observarse que existe muy poco rechazo al uso de nuevas tecnologías en las votaciones, sin embargo, a través de los comentarios realizados, es importante que se promueva la confianza en las instituciones y en las organizaciones que promueven el voto a través de este tipo de tecnologías.

BIBLIOGRAFÍA

UNIVERSIDAD PEDAGÓGICA NACIONAL, Introducción a los métodos estadísticos, vol. 2, México, Sistema de Educación a Distancia, Universidad Pedagógica Nacional, 1983.

PÁGINAS DE INTERNET

www.el-mundo.es/especiales/2002/10/internacional/brasil/urnas.html, agosto de 2004.

www.ieem.org.mx/ieem/numeralia/ieem_prep.htm, agosto de 2004.

www.yucatan.com.mx/especiales/constitucion/historia/asp, agosto de 2004.

www.ife.org.mx, agosto de 2004.

www.iedf.org.mx, agosto de 2004.

www.sepiensa.org.mx/contenidos/voto/voto1.html, agosto de 2004.

www.monografias.com/constitucion/voto/mujeres.htm, agosto de 2004.

Experiencia en el diseño de urnas electrónicas

UTILIZACIÓN DEL PROTOTIPO DE URNA ELECTRÓNICA

Lic. Marco Antonio Kalionchiz Rodríguez
Instituto Electoral y de Participación Ciudadana de Coahuila

Es licenciado en Derecho egresado de la Facultad de Jurisprudencia de la Universidad Autónoma de Coahuila. Actualmente realiza un Proyecto Empresarial sobre Urna Electrónica para obtener el grado de Maestría en Administración y Alta Dirección, y es director general del Instituto Electoral y de Participación Ciudadana de Coahuila, fue director jurídico y secretario técnico del anterior Consejo Estatal Electoral de Coahuila.

RESUMEN

La tecnología puede ser utilizada para facilitar todas las actividades del proceso electoral, por ello, el Instituto Electoral y de Participación Ciudadana de Coahuila, a partir del 2002, con ingenieros adscritos al mismo, ha desarrollado un prototipo de votación electrónica, a fin de dar cada día más confiabilidad y seguridad a la emisión del sufragio y a la obtención de resultados electorales definitivos. El proyecto de votación electrónica tiene por objeto la automatización del proceso de recepción del voto, para con ello simplificar las tareas de la jornada electoral, tales como apertura, cierre, escrutinio y cómputo de la casilla.

No se requiere capacitar de manera especial al elector para que pueda votar el día de la jornada electoral, toda vez que el *software* desarrollado es audiovisual y en todo momento conduce al elector en el proceso de votación. Además cuenta con una pantalla sensible al tacto lo que facilita su manejo haciendo que el proceso de votación sea sencillo, ya que el elector una vez que verificó su código de acceso, puede acceder a la boleta virtual para efectuar, con certeza y seguridad, la elección de su preferencia. El *software* desarrollado permite que los electores conozcan no sólo los nombres de los candidatos y de los partidos políticos que los postulan, sino también pueden ver la fotografía del candidato, existien-

do la posibilidad de incluir cualquier otra información que la autoridad electoral considere pertinente.

INTRODUCCIÓN

Es indudable que México está inmerso en un proceso de cambio en el que diariamente se fortalece la vigencia de ciertos principios y formas de vida, tales como el estado de Derecho, la democracia y la pluralidad política. En este proceso nos ha tocado participar a todos los mexicanos, particularmente a quienes tenemos la gran responsabilidad de formar parte de los órganos encargados de ejercer la función electoral en este país.

Hoy, la tecnología ha transformado la actuación de muchas actividades en el mundo, y nuestro país no es la excepción, es por eso que de igual forma los organismos electorales aplican distintas innovaciones a los procesos electorales.

Actualmente la informática ha tenido un gran impacto en la sociedad. El uso y desarrollo de las tecnologías de la información constituyen un instrumento de aprovechamiento que tiene la finalidad de elevar la competitividad de todos y cada uno de los sectores, y por ende, lograr el bienestar de toda la sociedad.

Cabe señalar que la tecnología desarrollada durante el siglo XX, especialmente los sistemas de cómputo, han alterado significativamente la forma en que se conducen las elecciones. El crecimiento de la población y el desarrollo de la democracia a lo largo del siglo XX han ocasionado que buena parte de la logística de las elecciones modernas dependa de la tecnología.

El desarrollo de la cibernética sirvió como base fundamental para la creación de prototipos en la implementación de la votación electrónica. Los avances en el diseño de computadoras continúan a un ritmo acelerado volviéndose indispensables para la vida cotidiana de cualquier país.

Una herramienta, que significa indiscutiblemente un avance en los procesos electorales, es la votación electrónica, mecanismo que ha sido desarrollado con gran éxito en otros países y que ha permitido hacer eficiente cada una de las tareas que conlleva la organización de una elección.

1. La votación electrónica

Actualmente, con el apoyo de la votación electrónica se tiene como objetivo dar mayor confianza al elector, celeridad a los procesos electorales y absoluta transparencia al sufragio.

En este contexto es importante mencionar que Coahuila en su ordenamiento electoral determina la posibilidad, como un precepto novedoso, de utilizar sistemas electrónicos y/o máquinas para recibir la votación el día en que tenga lugar la jornada electoral. Así el Artículo 171 de la *Ley de Instituciones Políticas y Procedimientos Electorales* para el Estado de Coahuila prevé que el modelo de los instrumentos electrónicos y/o máquinas que se utilice para recibir el voto deberá ser aprobado por el Consejo General del Instituto Electoral y de Participación Ciudadana de Coahuila, siempre que se garantice la efectividad y el secreto del sufragio.

En virtud de que la entrada en vigencia del ordenamiento en mención inició en noviembre de 2001, no fue factible utilizar sistemas electrónicos de votación para el proceso electoral que tuvo lugar en el 2002, dada la premura que implicaba, en ese entonces, su implementación.

Sin embargo, debido a este precepto y a que la tecnología puede ser utilizada para facilitar todas las actividades del proceso electoral, el Instituto Electoral y de Participación Ciudadana de Coahuila (IEPCC) ha realizado investigaciones respecto a la implementación de la tecnología en las elecciones, con el fin de dar cada día más confiabilidad y seguridad a la emisión del sufragio y la obtención de resultados electorales definitivos, así como la posibilidad de la votación de los mexicanos que se encuentren fuera del territorio nacional.

Hoy, a nivel mundial, no es una circunstancia exclusiva de nuestro país, existen opiniones encontradas respecto a las ventajas y desventajas que ofrece la votación electrónica, inclusive existen foros de discusión encargados de analizar el tema, como es el caso del Observatorio de Voto Electrónico. No obstante, no podemos desconocer que en muchos países del mundo ya se realizan con gran éxito procesos electorales con votación electrónica, entre otros: Venezuela, Costa Rica, Estados Unidos, el país Vasco y, de manera especial es el que representa Brasil, en donde en el 2000 el 100% de los electores emitió su voto mediante urnas electrónicas.

Y con ejemplos como estos podemos asegurar que incuestionablemente las bondades y beneficios que ofrece la votación a través de medios electrónicos son mayores que sus desventajas.

Cabe mencionar que ya en los procesos electorales existen incursiones en el terreno tecnológico, ejemplo de ello son los sistemas de resultados preliminares y los dispositivos de seguridad en las boletas electorales, que tanto el Instituto Federal Electoral (IFE) como los organismos estatales electorales utilizamos, por lo que no es complicada la implementación de este sistema.

2. Prototipo diseñado por el IEPCC

A partir de 2002, hemos desarrollado, con ingenieros adscritos al Instituto, un prototipo de urna electrónica, el cual surgió a raíz de las diversas investigaciones que realizamos, así como del estudio y análisis de los sistemas implementados en otros países; es importante señalar que se han diseñado diferentes prototipos que se han ido perfeccionando a fin de facilitar su manejo.

El proyecto de votación electrónica tiene por objeto la automatización del proceso de recepción del voto, para con ello simplificar las tareas de escrutinio y cómputo de las casillas. Este proyecto parte de dos premisas fundamentales: respetar el sistema de votación tradicional y, considerar la historia de nuestra cultura política. Por tal motivo, el diseño de votación electrónica surge de una combinación del sistema tradicional de votación con innovaciones tecnológicas.

El precepto legal coahuilense determina que deberá garantizarse la efectividad y el secreto del sufragio con la recepción del voto a través de medios electrónicos, pero es obvio que con un sistema de esta naturaleza invariablemente también tendrá que garantizar las características fundamentales del derecho al voto, que además de ser secreto, es universal, libre y directo.

En primer lugar la urna electrónica se caracteriza por su individualidad, ya que no tiene ningún vínculo con otras urnas ubicadas en otras casillas. Esto es, no están conectadas a ninguna red de comunicación.

No se requiere capacitar de manera especial al elector para que pueda votar el día de la jornada electoral, toda vez que el *software* desarrollado es audiovisual y en todo momento va acompañando al elector en el proceso de votación, contando con una pantalla sensible al tacto lo que permite facilitar su manejo. En este aspecto es de señalarse que para nosotros es muy claro que entre más sencillo sea el uso de la urna electrónica para el ciudadano, más invitado estará para participar.

Además, el proceso de votación es muy sencillo ya que el elector, una vez que verifique el código de acceso correspondiente, podrá acceder a la boleta virtual para realizar, con mayor certeza y seguridad, la elección de su preferencia. El *software* desarrollado permite que los electores conozcan no sólo los nombres de los candidatos y de los partidos políticos que los postulan, sino que también pueden ver la fotografía del candidato, lo que hace posible el incluir cualquier otra información que la autoridad electoral considere pertinente.

Con respecto a la secrecía del voto es importante señalar que los códigos de acceso al sistema se entregan de manera aleatoria, por lo que no es factible por ningún motivo identificar al elector con el código de acceso, ni mucho menos descifrar la información contenida en el mismo.

Por cuanto a la seguridad que ofrece este sistema: es auditable a través de cuatro vías, ya que cuenta con cuatro resguardos diferentes de información: dos electrónicos que consisten en el propio sistema y en un medio magnético removible y, los dos restantes son impresos, ya que el *software* está diseñado para que el elector una vez que emita su voto en la pantalla, obtenga impreso un comprobante de votación a efecto de que pueda corroborar su elección y lo deposite en una urna convencional.

Una característica más a destacar es la garantía de inviolabilidad ya que el sistema únicamente se podrá operar mediante dos códigos, uno de inicialización y otro de cierre, que estarán en poder de la persona que funja como presidente de la mesa directiva de casilla.

La mayoría de las personas pueden pensar que todo eso está muy bien para los países desarrollados, pero ¿qué hay de los países en desarrollo sin la infraestructura apropiada? Incorporar nuevas tecnologías para propósitos electorales puede incrementar los costos o disminuirlos depen-

diendo del financiamiento de la nueva tecnología en comparación con el del sistema al que reemplaza. La tecnología puede parecer costosa en la etapa de implantación, sin embargo, puede ahorrar dinero a mediano plazo, y permite estar al alcance de cualquier persona en cualquier lugar del mundo.

Como consecuencia de las características con que cuenta el prototipo, se comprueba que las ventajas que aporta el sistema electrónico son muchas, ya que se simplifican los procesos de apertura y cierre de casillas, así como el de votación; no existen errores ni omisiones en el llenado de las actas, no hay votos nulos, se omite el escrutinio de las boletas, los resultados finales se realizan en corto tiempo y se profesionaliza la labor de los funcionarios de las mesas directivas de casillas, reduciendo el número de los mismos.

Por otra parte, la tecnología mejora con tal velocidad que la de hoy puede ser caduca para cuando se organice una próxima elección en tres o cuatro años. Por tal motivo, el IEPCC, continúa en el estudio y la investigación de los sistemas electrónicos, y el perfeccionamiento del prototipo diseñado. Se ha disminuido su peso y su tamaño, igualmente se ha mejorado el material con el que se construye la urna electrónica.

3. Presentación y aplicación de la urna electrónica

Este proyecto se ha presentado ante autoridades federales y locales, ha contado con mucha aceptación por parte de las mismas. Actualmente hemos tenido la oportunidad de apoyar con este instrumento a algunas instituciones educativas, partidos políticos y organismos electorales estatales en diversos procesos electorales, con gran éxito en su implementación.

En marzo de 2003 hicimos la presentación oficial del prototipo de la urna electrónica a la sociedad coahuilense, en donde contamos con la presencia del procurador general de la República, Rafael Macedo de la Concha, los titulares de los tres Poderes del Estado, la titular de la Fiscalía Especializada para la Atención de los Delitos Electorales, autoridades del IFE, representantes del Tribunal Electoral del Poder Judicial de la Federación, alcaldes, diputados, representantes de partidos políticos, directores

de instituciones educativas, dirigentes de cámaras y organismos no gubernamentales, notarios públicos, entre otros.

Asimismo, es importante mencionar las presentaciones del proyecto de votación electrónica y las aplicaciones que ha tenido la urna electrónica desarrollada por el IEPCC, tales como:

Presentaciones:

- El 8 de abril de 2003 en las instalaciones del IFE ante autoridades de dicho organismo.
- En el Consejo Lagunero de Iniciativa Privada, en la ciudad de Torreón, Coahuila.
- En Veracruz en la sede del Tercer Encuentro Nacional de Consejeros Electorales los días 22, 23 y 24 de mayo de 2003.
- El 16 de junio del 2003 ante el representante designado por el presidente de la República, Vicente Fox Quesada, José Francisco Paoli Bolio, subsecretario de Desarrollo Político de la Secretaría de Gobernación.
- El 18 de junio de 2003, en "El Foro Nacional Democrático de México", realizado en la ciudad de Monterrey, Nuevo León.
- El 27 de junio de 2003 ante el secretario de Gobernación el Lic. Santiago Creel Miranda en su pasada visita a la ciudad de Saltillo, Coahuila.
- En el estado de Aguascalientes el 24 de septiembre de 2003 ante el Instituto Estatal Electoral de Aguascalientes, el Congreso del Estado y ante el Ejecutivo de esa entidad federativa.
- El 17 y 18 de octubre de 2003, en Tabasco en el marco de la sesión ordinaria de la Asamblea General de la Asociación Nacional de Universidades e Instituciones de Educación Superior.
- El 20 de enero de 2004, la urna electrónica en Sonora en la I Jornada para la Cultura Democrática, organizada por el consejo estatal electoral de ese estado.

Aplicaciones:

- Los días 17, 18, y 19 de junio de 2003, se llevó a cabo un ejercicio con el proyecto de Votación Electrónica de Coahuila, en el marco de "La Jornada Juvenil Electrónica", que tuvo lugar en Chiapas.
- A raíz de las bondades que ofrece este sistema de votación electrónica, la Universidad Autónoma de Coahuila, máxima casa de estudios de nuestra entidad, solicitó la suscripción de un convenio de colaboración con el Instituto Electoral y de Participación Ciudadana de Coahuila para realizar a través de la urna electrónica las elecciones de directivos de escuelas y facultades que decidieran optar por este sistema de votación. Así, con gran éxito se llevó a cabo la elección de Director en la Escuela de Odontología de la Universidad Autónoma de Coahuila el 5 de septiembre de 2003.
- De igual forma se utilizó en la elección de Director de la Facultad de Jurisprudencia de la Universidad Autónoma de Coahuila en la primera ronda el 2 de octubre de 2003 y en la segunda ronda de la elección el 6 de octubre.
- El 25 de octubre de 2003 se llevó a cabo la elección de Director en la Facultad de Ciencias Políticas y Sociales de la Universidad Autónoma de Coahuila.
- El 1 de diciembre de 2003, se utilizó igualmente la urna electrónica en la elección de Director de la Escuela de Música de la Universidad Autónoma de Coahuila.
- El ejercicio de elección de 72 miembros del Consejo Estatal y 20 miembros del Consejo Nacional del Partido Acción Nacional en el estado de Nuevo León, el 18 de abril de 2004.
- El 25 de mayo de 2004, se llevó a cabo la elección de Director en la Escuela de Bachilleres Dr. Mariano Narváez, turno vespertino de la Universidad Autónoma de Coahuila.
- En el Programa de Elecciones Infantiles 2004 en el estado de Chihuahua, en dos etapas, una el 27 de junio en 15 diferentes municipios de Chihuahua y la otra el 4 de julio en Ciudad Juárez y en la ciudad de Chihuahua. El *software* instalado para este ejercicio fue hecho en tres

diferentes lenguas, español, alto tarahumara y bajo tarahumara, lo cual permite mayor facilidad en su comprensión.

- El 9 de septiembre de 2004 se llevó a cabo la elección de miembros de la Asociación de Estudiantes y del Consejo Universitario en la Facultad de Ciencias Políticas y Sociales de la Universidad de Querétaro.
- El 22 y 23 de septiembre de 2004 se celebró la elección de Consejeros Universitarios en la Universidad de Guadalajara, para lo cual se suscribió previamente, el 17 de junio de ese año, un convenio con dicha universidad.

4. Conclusiones

Por lo antes expuesto, el sistema de votación electrónica es sin duda un paso importante para la automatización y simplificación de los procesos electorales, y al relacionarlo con otros sistemas electrónicos que actualmente representan un progreso representativo, nos damos cuenta que los organismos electorales no podemos sustraernos, en la función que tenemos encomendada, al desarrollo tecnológico que día a día se va incorporando en el mundo.

Como consecuencia de las características con que cuenta el prototipo se comprueba que las ventajas que aporta el sistema electrónico son muchas, ya que se simplifican los procesos de apertura y cierre de casillas, así como el proceso de votación, no existen errores ni omisiones en el llenado de las actas, no hay votos nulos, se omite el escrutinio de las boletas, los resultados finales se realizan en corto tiempo y se profesionaliza la labor de los funcionarios de las mesas directivas de casillas, reduciéndose el número de los mismos.

Por otra parte, la tecnología mejora con tal velocidad que la de hoy puede ser caduca para cuando se organice una próxima elección en tres o cuatro años, por tal motivo, el Instituto Electoral y de Participación Ciudadana de Coahuila continúa y continuará con el estudio e investigación de los sistemas electrónicos, para afinar paulatinamente el prototipo diseñado.

La urna electrónica brasileña y la cultura del fraude

Mario Ortega Olivares
Universidad Autónoma Metropolitana (UAM)

Es profesor en el Departamento de Relaciones Sociales de la UAM, unidad Xochimilco. Tiene estudios de doctorado en la Escuela Nacional de Antropología e Historia. Entre sus publicaciones destacan: *La Utopía en el Barrio; Productividad y Fatiga Laboral; Octubre Dos, Historias del Movimiento Estudiantil*. En 1991 recibió el Premio Nacional de Investigación Urbana y Regional.

RESUMEN

Se comentan los requisitos básicos que debe cumplir una urna electrónica para reemplazar a la urna convencional. Se discuten las diferencias entre las urnas de lectura óptica del voto y las de registro electoral directo, ya sea que usen teclado, pantalla sensible al tacto o tarjeta de chip. Se presentan las mejoras propuestas para la urna brasileña. Se hace la recomendación para el diseño de la urna en nuestro país. Además se considera que la urna electrónica en México podrá eliminar muchas de las operaciones irregulares acostumbradas en nuestra cultura política.

INTRODUCCIÓN

Se encuentra en marcha una revolución en las telecomunicaciones digitales que transformará la vida política democrática a escala global. Esta revolución proyecta que: Los partidos políticos difundirán sus programas en línea; los ciudadanos residentes en el extranjero votarán por Internet; las minorías étnicas, analfabetos y discapacitados superarán, con herramientas electrónicas, las barreras que restringen su participación; y el gobierno electrónico será muy sensible a la opinión pública gracias a las consultas y a los referendos en urnas electrónicas.

1. El simulacro mexicano con la urna electrónica

En 2003, el Instituto Electoral del Distrito Federal (IEDF) firmó un convenio marco para el desarrollo de una urna electrónica con tecnología mexicana, para lo cual integró un Comité Técnico con la participación de la Universidad Autónoma Metropolitana, la Universidad Nacional Autónoma de México, el Instituto Politécnico Nacional y el Instituto Tecnológico de Estudios Superiores de Monterrey.

El 6 de julio del mismo año, con la asesoría del Tribunal Superior Electoral (TSE) de Brasil, se realizó en la Ciudad de México, un simulacro de votación electrónica paralelo a las elecciones federales, en el que participaron más de 23 mil ciudadanos, quienes además de votar en urnas convencionales, hicieron lo propio en las electrónicas. Más de 91% de las 22 713 personas que respondieron el cuestionario de salida: consideraron que "es sencillo usar las urnas electrónicas y que son claras las instrucciones de operación".[84] También dijeron estar de acuerdo en emplearlas en próximas elecciones.

Entre los objetivos del simulacro, el consejero presidente del IEDF, Javier Santiago Castillo, incluyó derribar la resistencia cultural de los ciudadanos a usar las nuevas tecnológicas digitales, que además de: "abaratar los costos del proceso, tienen como beneficio la desaparición de causales de conflicto, errores de suma, valoraciones sobre la validez de los votos, pero sobre todo, demostrar la transparencia en el manejo de los resultados electorales".[85]

Entre el 12 de septiembre y el 1 de octubre de 2003 el IEDF efectuó otra prueba piloto con la urna electrónica, donde participaron más de 56 mil estudiantes de 160 planteles de nivel medio superior en el Distrito Federal. Uno de los resultados de este ejercicio resaltó que: "corrupción e ineficiencia fue creciente respecto al grado escolar".[86]

---

[84] Leonardo Valdés, "Vote Station", *Voz y Voto*, número 129, noviembre de 2003.

[85] Juan José Galván, "Apoya la urna electrónica procesos democráticos", http:www.ccm.itesm.mx/noticias/jaque/urna.html, 15 de julio de 2004.

[86] Instituto Electoral del Distrito Federal, "Resultados de pruebas piloto con urnas electrónicas", *Urna*, número 29, año 5, mayo de 2004.

2. Requisitos para una urna electrónica

Cuando se analiza la viabilidad de una urna electrónica se deben contemplar los siguientes objetivos esenciales:

Respetar el derecho al voto universal, libre, secreto y directo, alcanzar la mayor participación de los ciudadanos y ciudadanas, y asegurar la transparencia del proceso electoral.

Si la urna electrónica ha de reemplazar a la urna convencional, al menos debe ofrecer las mismas ventajas que está última y, si es posible, superarla. Debe garantizar la seguridad suficiente para que los electores emitan su voto en completa libertad y en privado, sin que exista la posibilidad de ser influenciados o coaccionados. Es indispensable que la identidad del elector no pueda ser asociada con el partido por el que sufragó, pues el secreto del voto es esencial a la democracia. Se recomienda que la identificación del elector y el registro del voto ocurra en equipos diferentes que no estén conectados entre sí, para eliminar la posibilidad de asociar al ciudadano con su preferencia electoral.

La nueva urna debe garantizar que todos los ciudadanos con derecho a voto lo puedan ejercer, lo cual es muy importante en un país pluriétnico y multicultural. En las últimas décadas se ha incrementado la cantidad de hablantes de lenguas indias que residen en la capital. La urna no debe presentar barreras para el voto de personas con capacidades distintas o analfabetos.

Tras la validación de la urna electrónica por parte de la autoridad electoral, sería conveniente su certificación por organismos no gubernamentales y por técnicos de los partidos políticos interesados. Por ser una urna pública, el sistema de votación debe estar a la disposición de quien quiera comprobarlo, en todo momento y bajo cualquier circunstancia. Por eso se recomienda emplear sistemas operativos de libre uso. El sistema debe asegurar que los votos no puedan ser alterados, modificados o suprimidos. El principio democrático de que a cada persona le corresponde un voto, significa que todos los votos sufragados sean contados.

Nada apoyará más la confianza de los electores, que la posibilidad de auditar los resultados emitidos en la urna electrónica. La experiencia

internacional señala la necesidad de contar con registros en papel que faciliten la certificación de las cuentas electorales.

3. ¿Qué es una urna electrónica?

Hay dos tipos de urnas electrónicas de Registro Electrónico Directo (RED), una dotada con una pantalla sensible al tacto, y otra con un teclado numérico. En la urna RED del primer tipo, la pantalla exhibe la foto del candidato y su partido, el votante elige al de su preferencia marcándolo con su índice o con un lápiz electrónico directamente en la pantalla.

En la urna RED con teclado numérico la diferencia consiste en que cada candidato es identificado por un dígito, que debe oprimirse en el teclado, como lo hacemos en los cajeros automáticos bancarios. Inmediatamente después la urna presenta la foto y el logotipo del partido, para confirmar o corregir la selección. Después de que el elector oprime la tecla para aceptar el voto, este es validado y se graba en la memoria. Al igual que en los otros casos, se imprimen los resultados y el acta. Para transmitir después los resultados al computador central.

Otros sistemas cuentan con pantallas sensibles al tacto y una impresora que emite un *ticket* como respaldo documental del sufragio.

4. La urna electrónica brasileña

En las elecciones presidenciales de 2002 en el Brasil, donde ganó el candidato opositor Lula da Silva, 115 millones de electores emitieron su sufragio en más de 406 mil urnas electrónicas. Son del tamaño de una caja registradora de supermercado, y fueron desarrolladas a iniciativa del TSE de ese país. El programa de *software* empleado fue diseñado por el TSE con el apoyo del corporativo Microbase, quien aportó el sistema operativo VirtuOS, compatible con Windows. Y de Procomp, quien se encargó del *software* de aplicación.

La microterminal de la urna electrónica tiene una pantalla y un teclado telefónico con números y botones: blanco para escoger; verde para confirmar el voto y rojo para corregirlo. Cuenta con marcas para invidentes y una unidad de sonido que comenta al elector lo que se mira en pantalla. Además cuenta con una tarjeta *flash*, o memoria de lecto-

escritura que almacena el *software* básico con los datos de los candidatos y sus partidos, así como el padrón electoral local. Y otra *Flash Card* desmontable con los archivos complementarios para operarla; los datos se pueden transferir en disco.

Al iniciar las labores de la casilla, cada equipo debe emitir la *zerésima* o constancia de que el sistema está en ceros. En el momento de la votación, el ciudadano oprime el número del candidato preferido y confirma si no hay necesidad de corrección. Sin embargo, cuando se juntan las elecciones locales, provinciales y federales son muchos números que pueden confundir al elector, por eso: "las autoridades recomendaban llevar los números anotados en una especie de chuleta [acordeón] electoral",[87] con los números de los candidatos a apoyar.

Cuando el ciudadano termina aparece un letrero de fin. Se enciende un indicador señalando que la urna está libre, pero no puede usarse hasta que lo autorizan los fiscales electorales. Después el elector se retira con su constancia de voto, pues en Brasil el voto es una obligación y se multa a quien no cumple. Cuando terminan las votaciones el fiscal de la casilla digita su clave o *password* para cerrar la computadora e imprimir los resultados.

5. Propuestas para mejorar la urna brasileña

Para aumentar su confiabilidad, el Observatorio Electoral, una organización no gubernamental brasileña, propuso una auditoría por muestreo estadístico de las urnas electrónicas. "Como la carga del programa básico se realiza por parte del proveedor de la urna, los controles deben hacerse al momento de ser entregadas para poder cargar los software de aplicación, o sea el que contiene los datos con las listas de los partidos y candidatos para cada circunscripción, una auditoría completa, no estadística, para llegar a errores cero, que permita asegurar a todo contendiente que todo está en orden, requiere un número de técnicos y horas de trabajo importantes, que no están al alcance de ningún partido político

[87] El Mundo, "El nuevo presidente de Brasil es..." Caetano Veloso, www.el-mundo.es/especiales/2002/107internacional/brasil/guerraboton.html, 15 de julio de 2004.

[...] Habría que recurrir a técnicos contratados, lo que tampoco es factible dado los costos de esa actividad. Una alternativa es una auditoría en base a principios probabilísticos [...] Esa auditoría independiente debería ser realizada por una comisión técnica. La misma debe contar con miembros de los partidos políticos y eventualmente de organizaciones de la sociedad civil que trabajen en el tema de la participación ciudadana [...] Las máquinas deben ser auditadas antes del proceso electoral para determinar que están en cero, deben ser cargadas con el software de aplicación en la hora indicada para hacerlo y deben seguirse todos los procedimientos previstos".[88]

6. Críticas a la urna electrónica de Brasil

Pero en este mundo no hay nada perfecto, Osvaldo Manechy,[89] un reconocido periodista de Río de Janeiro asegura que la urna electrónica no es infalible. Para comprobarlo documentó irregularidades en las elecciones del 2002. Como el sonado caso de *Aroçoiaba da Serra*. Todo comenzó cuando los encargados del patrón electoral local omitieron cargar en la urna electrónica, el nombre y la foto de candidatos a consejeros municipales del Partido Trabalheiro (PT). El problema es que nadie se percató de ello. Para los funcionarios electorales y de partido, ilusionados con las maravillas de la urna: la carga de datos, la prueba y el lacrado de las urnas era una simple formalidad sin sentido, por lo que el problema continuó.

El día de las elecciones, los electores descubrieron un error en la urna electrónica, porque al oprimir el número de sus candidatos, la máquina respondía que el voto sería anulado. Mandaron llamar al juez, quien instruyó a los electores que querían votar por los candidatos del PT para que regresaran a las 16:00 horas, violando el secreto del voto. Al volver los electores para votar por los candidatos del PT, se les dijo que votaran en blanco en la urna electrónica y luego emitieran su voto en una cédula

[88] Juan Rial, "Los sistemas y máquinas disponibles", www.observatorioelectoral.org/biblioteca/?bookID=26&page=8, 15 de julio de 2004.

[89] Osvaldo Manechy, "Plam Beach versus Araçoiaba da Serra", eee1.jus.com.br/doutrina/texto.asp?id=1553, 15 de julio de 2004.

de papel, cuando hizo el recuento resultó que había más votos para consejeros que electores.

El juez decidió anular los votos en papel y validar los votos electrónicos para consejeros, a pesar de que ordenó que se votara en blanco en las urnas electrónicas. Los candidatos del PT registraron cero votos. Para zafarse del problema, el juez electoral inventó una modalidad jurídica, el voto *desconsiderado*, ignorando así los votos emitidos en papel. Los afectados presentaron un recurso legal, pero por las peculiaridades del sistema electoral brasileño, el caso fue resuelto por el mismo juez del problema. Obviamente desechó la petición. El Tribunal Regional Electoral también declaró improcedente la queja. Finalmente las elecciones fueron anuladas por el TSE, después de un tortuoso proceso que puso en duda la imparcialidad de la justicia electoral brasileña.

Kim asemeja a la urna electrónica, por no emitir comprobante con: "el dictado del voto a una persona que se encuentra oculta tras una cortina y toma nota del mismo. El votante no tiene manera de saber si el escriba registró el voto correctamente".[90] De ahí la propuesta de que la urna imprima un *ticket* auditable, que se deposite en una urna transparente sin intervención de manos humanas.

Otra precaución que espero sea tomada en cuenta en el diseño de la urna electrónica mexicana, es el uso de sistemas operativos libres como es el caso de Linux u otros semejantes, para que los ciudadanos interesados y calificados, puedan certificar tanto los programas como el código fuente, es decir el *software* utilizado. En los Estados Unidos, tras el escándalo del estado de Florida hay toda un polémica al respecto:

7. La mejor defensa de la urna electrónica es someterla a prueba

Un grupo de brasileños expertos en seguridad digital del *Fórum do Voto Eletronico*, redactó esta lista de puntos críticos en las elecciones electrónicas:

[90] Kim Zetter, "Buscan estándares para la votación electrónica", Wired News, ar.wired.com/wired/politics/0,1156,25581.html, 11 de julio de 2004.

a) Fantasmas: si algún funcionario corrupto registra personas inexistentes, es muy difícil descubrirlo. Una solución posible es realizar auditorías a los padrones.

b) Errores humanos: en el caso de *Araçoiaba da Serra* no falló el programa del TSE, sino los técnicos que no incluyeron a ciertos candidatos.

c) El tiempo para validar es corto: los fiscales argumentan que el tiempo es insuficiente para analizar si el programa puede desviar votos.

d) Dificultades en la verificación: los fiscales de los partidos pueden simular algunos votos para comprobar que no hay desvíos; pero consideran simple el procedimiento, al compararlo con las posibilidades de adulteración. Piden acceso a la *Flash Card* que instala en las urnas el sistema operativo de votación, los datos de los candidatos y los números de los electores para cada sección, con dos meses de anticipación.

e) Falta de transparencia: los técnicos consideran que por ser una urna pública, no hay razón para emplear un programa secreto de criptografía. Una propuesta es remplazarlo por un diseño digital, que es más laborioso pero más transparente.

f) Dificultades en el recuento: en una urna electrónica no se pude comprobar cada voto.

g) La violación del secreto: un programa clandestino podría registrar el nombre de los electores y el partido que eligieron. Los críticos proponen que la urna y la lista de votantes sea registrada en una máquina diferente.

h) Programa abierto: a diferencia del código fuente de Windows, un programa abierto como Linux, permitiría la fiscalización del sistema.

i) El chip puede ser regrabado: el *Bios* de la urna es regrabable y puede ser alterado para incluir un programa ladrón de votos.

j) Clonación del disco: un disquete alterado puede grabarse en una urna clonada o una urna oficial, si el defraudador cuenta con los datos para ajustar el reloj. Pues el disco registra los votos de la sesión, indica cuáles electores votaron y cuántos faltaron, además de que registra el horario de funcionamiento de la urna.

k) Alteración del total: un técnico con acceso a la red del TSE puede defraudar el proceso. Una forma de evitarlo es comparar uno a uno los

resultados, con la suma total fijada en la puerta de cada sección. Pero los fiscales alegan que no da tiempo y que el problema se resolvería, si el sitio *web* del TSE publicara los boletines de todas las secciones en tiempo real.

l) Tiempo escaso: "los fiscales no consideran a la rapidez de operación como un factor positivo, pues los presiona al trabajar. La ley electoral establece un plazo de 48 horas para presentar impugnaciones".[91]

El profesor Rezende de la Universidad de Brasil, opina que la línea fronteriza entre la seguridad y la transparencia es engañosa. Por un lado, el secreto del *software* protege al TSE contra el fraude externo, pero desde la otra cara de la moneda, lo deja expuesto al fraude interno. Procedamos a ver la discusión en México.

8. La cultura del fraude en México

El fraude en los comicios es una desafortunada práctica que forma parte de la cultura política en todo el mundo y lastima la confiabilidad de las elecciones, México no es una excepción. La singular cultura política mexicana fue investigada primeramente por Gabriel Almon y Sidney Verba en su obra clásica *La Cultura Cívica,* que fue publicada en 1963 por la Universidad de Princenton. Aunque las formas culturales con las que se manifiesta el fraude en México es muy singular, se debe reconocer que hasta los países con las democracias más desarrolladas, como los Estados Unidos, padecen este mal. Grag Palast, reportero del periódico *The Guardian,* denunció que en las elecciones de 2000, el Estado de Florida contrató a la empresa "DBT" para depurar del padrón a los delincuentes inhabilitados para votar. Pero la lista fue ampliada con personas inocentes, cuyos nombres fueran similares a los de los infractores, o que tuvieran la misma fecha de nacimiento.

En el senado brasileño, el 23 de mayo de 2001 se abrió el proceso de destitución de dos senadores, Carlos Antonio Magalhaes y José Roberto

[91] Rafael García, "Hackers do voto", *Revista Galileo,* revistagalileo.com/Galileu/0,6993,EC-T328480-1719,00.html, 17 de julio de 2004.

Arruda, por haber violado el secreto del panel electrónico de la cámara, durante una votación: "Arruda sostuvo que no ordenó la violación del procedimiento, sino que se limitó a indagar por curiosidad a la funcionaria sobre la posibilidad de identificar a los autores de cada voto en una sesión secreta".[92] Incluso el famoso carrusel, que podríamos considerar exclusivo de nuestro folklore político, existe en Colombia: "un grupo de aparentes votantes circula como un carrusel por los lugares de votación, le muestra a los jurados fletados cualquier cédula, recoge los tarjetones que éstos les entregan en cada pasada y proceden tranquilamente, una y otra vez, a marcarlos y depositarlos en las urnas".[93]

El uso de la urna electrónica en México, como ha ocurrido en otras experiencias de innovación digital, lanzará al desempleo por analfabetismo tecnológico a los llamados *mapaches*, nombre con el que se designa popularmente a los caciques expertos en el fraude electoral. Antes de discriminar cuáles formas de fraude serán desplazadas por la urna electrónica, daremos un breve repaso a las prácticas fraudulentas presentes en la cultura política mexicana, descritas por Aparicio y coautores:

a) El *Carrusel* o la *Brigada*: consiste en el acarreo de votantes con la finalidad de que voten por el partido de quienes organiza el fraude.
b) El *Rasurado* del Padrón Electoral: se eliminan del padrón electoral los nombres de un cierto número de ciudadanos que pueden votar por el partido opositor al de los defraudadores.
c) *Ratones locos*: los votantes van de una casilla a otra en busca de la que les corresponde, pues funcionarios corruptos, sin previo aviso les cambian la casilla en la que les correspondía votar.
d) Operación *Tamal*: el día de las elecciones se organizan desayunos masivos para que los comensales vayan a votar por el partido de los fraudulentos.

[92] El Día, "Golpe demoledor al oficialismo en Brasil", Edición Internacional, 200.26.207.200/ediciones/20610524/elmundo4.esp, 24 de mayo de 2001.

[93] Arturo Sarabia, "Radiografía del fraude electoral", www.terra.com.co/elecciones2003/informes_especiales/analisis/16-10-2003/nota112963.html, 15 de julio de 2004.

e) Operación *Manitas*: Se violan los paquetes electorales para alterar su contenido.
f) *Tacos* de Boletas o *urnas embarazadas*: las urnas se rellenan con paquetes de boletas cruzadas a favor del partido de los tramposos.
g) Fraude *Hormiga*: las mesas directivas de casilla permiten la violación generalizada de las leyes electorales, votan ciudadanos sin credencial y los que no aparecen en las listas nominales.
h) Fraude por *Votos a cambio de ayuda*: El acceso a los programas sociales se condiciona, a la entrega de votos a favor del partido que los controla a nivel local.
i) *Fraude cibernético* o *Ingeniería Electoral*: Manipulación de cifras, padrón, credenciales, listas nominales, etcétera, desde el sistema computarizado[94] para beneficiar al partido de quienes realizan el fraude.

Está tan arraigada la cultura del fraude electoral en México que Gómez Tagle en su investigación sobre las elecciones de 1979, 1982 y 1985, encontró que en muchos lugares donde hubo fraudes o irregularidades por parte del partido político que mantenía la hegemonía por aquellos días, se realizaron fraudes en los que dicho partido político: "hubiera triunfado de cualquier manera".[95]

En una encuesta de opinión al respecto realizada en 1994 se encontró que:

"La variación en la percepción del fraude es sumamente significativa no sólo entre una elección y otra (para 1988 casi la mitad opina que hubo fraude, mientras que en 1991 son poco menos de la cuarta parte), sino fundamentalmente entre la creencia general y en abstracto de que sí hay fraude en México, y la más baja para una elección en particular (1991), y la notablemente inferior para la elección de 1994. La primera percepción remite más a la creencia generalizada de que se comete fraude en

[94] Diana Aparicio, Enrique Guzmán y Javier Guzmán, *La legislación electoral y el diseño del fraude en la cultura política mexicana*, México, Facultad de Ciencias Políticas y Sociales UNAM, 1997.

[95] Silvia Gómez Tagle, *Democracia y poder en México: el significado de los fraudes electorales en 1979, 1982,y 1985*, Nueva Antropología, 9 (3) 1986.

México, con toda la carga de estigmatización que la suposición de este ilícito conlleva; por el contrario, las otras estimaciones aluden más a la experiencia concreta".[96]

Con motivo de la controvertida "caída del sistema" en dichas elecciones de 1988, se documentaron al detalle las irregularidades encontradas. Las cuales incluyeron desde el falseamiento del padrón y el rellenado de urnas, hasta la alteración de resultados en el acta electoral, en este segundo caso se pueden seguir las siguientes variantes:

a) Se reelabora por completo el acta electoral, de tal manera que los números que aparecen registrados, con la cantidad de votos para cada partido político y los votos anulados son falseados.
b) Se añade un dígito a la derecha de la cifra de votación total del partido favorecido, con lo que se multiplica aproximadamente 10 veces. (Por ejemplo: un resultado de 358, al añadirle un 9; se convierte en 3 589).
c) Se añade un número a la izquierda de la cantidad real, para agregar desde cien hasta miles de supuestos votos. (De esta manera, un 416, al agregarle un 7 a mano izquierda; se transformar como por arte de magia en 7 416).
d) Si la primera cifra del resultado es un número uno; basta con alterarlo para: "hacer un cuatro, un siete, o un nueve a partir de un uno".[97] Práctica común con las boletas de calificación. Aunque no todas las irregularidades en el conteo son resultado de manipulaciones, muchas provienen de errores en las sumas aritméticas.

9. La urna electrónica y el adiós a los *mapaches*

Como puede apreciarse, muchas de estas trampas podrán ser eliminadas con la introducción de la urna electrónica. Si los datos se registran en

[96] Ángela Giglia y Rosalía Winocur, "Posibilidades y alcances de las técnicas antropológicas para el estudio de la cultura política", *Algunos enfoques metodológicos para estudiar la cultura política en México*, México, IFE-FLACSO-Porrúa, 2002.

[97] José Barberán, Cuauhtémoc Cárdenas, Adriana López y Jorge Zavala, *Radiogr Fraude. Análisis de los datos oficiales del 6 de julio*, México, Nuestro Tiempo, 1988.

las tarjetas de memoria de la urna digital, ninguno de los cuatro tipos de alteración numérica de resultados descritos arriba podrán realizarse, ya que el acta la emite la urna electrónica automáticamente.

Lo mismo sucederá con la operación *Manitas*, pues no se podrán violar las urnas electrónicas para alterar su información. La costumbre de introducir boletas enrolladas como *Tacos*, también entrará en desuso, pues los votos electrónicos son dígitos inmateriales. Lo propio ocurría con las *urnas embarazadas*, pues las electrónicas emiten un certificado de cuenta en cero, al que los brasileños ha nombrado la *zerésima*. El fraude *hormiga* tan socorrido por los caciques urbanos y campesinos se evitará. Si algún funcionario intenta permitir el voto de quien no esté registrado, o no presente su credencial con banda magnética, la urna electrónica lo rechazará. Por ello adquirirá más importancia la transparencia y auditoría del padrón electoral y de los programas del *software* de la urna y del centro nacional de cómputo.

10. Conclusiones

Podríamos remarcar la conveniencia de que los diseñadores de la urna electrónica mexicana utilicen un sistema operativo libre, que no se encuentre protegido por una patente comercial para facilitar su auditoría. Para seguir la tendencia internacional, será conveniente que la urna cuente con una impresora que emita un comprobante en papel o *ticket* que se deposite sin la intervención de manos humanas. Debe evitarse el error de las autoridades brasileñas, quienes presentaron a la nueva urna como infalible y 100% segura, sin matizar sus fortalezas y debilidades. Pues tal tipo de propaganda en lugar de favorecer su aceptación pública, la comprometen con metas imposibles de alcanzar.

Sin duda la urna electrónica será un importante avance para la democracia en México, pues desplazará del proceso de control y conteo de votos a los obsoletos caciques electorales, que han medrado de manera clientelar con el voto de la gente que necesita el apoyo de programas sociales. Pero como nada es perfecto, surgirá un nuevo riesgo, el del fraude electrónico. Técnicos de alto nivel podrían, desde el interior del aparato electoral, desarrollar programas de *software* para desviar o alterar los votos

en la urna electrónica, como los llamados *caballos de Troya*. Queda por resolver el dilema de la impresión en papel de los votos, pues al hacerlo se podría desatar una cascada de impugnaciones sobre la validez de los resultados emitidos. Nuestro reto es abrir camino al siguiente paso evolutivo de la democracia en México: la democracia electrónica.

BIBLIOGRAFÍA

PYE, Lucien W. y Sydney Verba, "Political Culture and Political Development", Estados Unidos, Princenton University Press, 1965.

MINISTERIO DEL INTERIOR DE ARGENTINA, *Fortalezas y debilidades de los sistemas electrónicos de votación, Documento de discusión interna 1*, Argentina, Ministerio del Interior, 2004.

WINOCUR, Rosalía, *Algunos enfoques metodológicos para estudiar la cultura política en México*, México, IFE-FLACSO-Porrúa, 2002.

PROBLEMAS Y SOLUCIONES EN LOS SISTEMAS AUTOMATIZADOS DE VOTACIÓN[98]

Lic. César Flores Zavarce
Universidad Católica Andrés Bello
Caracas, Venezuela

Es sociólogo por la Universidad Católica Andrés Bello. Cursó estudios de Socioeconomía en Alemania, en las universidades de Munich y Augsburgo, y formó parte del Programa Galileo de la Fundación Gran mariscal de Ayacucho.

Actualmente es coordinador de Pre-Venta y Operaciones de la empresa Smartmatic, donde es responsable de manejar los mercados venezolano y colombiano en el tema de automatización electoral.

En el ámbito de la consultoría gerencial, ha realizado proyectos a nivel nacional e internacional, y sus principales contribuciones han sido en las áreas de Planificación Estratégica, Desarrollo Organizacional, Reingeniería de Procesos, Gerencia del Cambio y Gerencia del Conocimiento.

RESUMEN

El uso de los sistemas automatizados de votación ha generado en varios países denuncias de escándalos y fraudes. En este artículo se analizan los principales problemas de los sistemas automatizados de votación; las limitaciones los riesgos que representan, y de cómo estos problemas son resueltos con la automatización de elecciones SAES de Smartmatic.

[98] Material elaborado por Product and Marketing Department Smartmatic Corp.
Con sede en Florida, Estados Unidos, y con oficinas en México y Venezuela, Smartmatic es una compañía multinacional especializada en la creación y despliegue de soluciones de alta seguridad y conectividad, y es el líder mundial en tecnología y servicios de automatización electoral.
Smartmatic Automated Election Systems (SAES), es la solución de automatización electoral ya que constituye el sistema integral de votación más seguro, confiable y auditable del mundo.
Smartmatic es propietario de Sequoia Voting Systems, empresa líder en sistemas de votación electrónica en el mercado estadounidense, lo cual le permitió consolidarse como el líder global indiscutible en el despliegue de sistemas y servicios de automatización electoral a nivel mundial.

INTRODUCCIÓN

La automatización de los procesos electorales es una creciente tendencia mundial: en los últimos cinco años y de manera casi simultánea, países de Latinoamérica, Europa y Asia han implementado de forma parcial o total distintas modalidades de sistemas de votación automatizado con miras a realizar importantes ahorros en costos, agilizar la obtención de resultados y reducir los riesgos de fraude en el proceso electoral.

Países como Paraguay, Suiza, Bélgica, Brasil y Australia, entre otros, comprueban con hechos recientes los puntos a favor de los sistemas automatizados de votación (SAV, por sus siglas en español). Sin embargo, no todas las experiencias relacionadas con el uso de sistemas de votación automatizados han sido positivas. En algunos países como Estados Unidos e Irlanda, las historias de fraudes y escándalos relacionados con las limitaciones de estos sistemas ponen seriamente en entredicho el uso de los SAV, llegando inclusive al punto de sacar de circulación miles de máquinas de votación automatizadas ya adquiridas, por haber demostrado porcentajes de fallas superiores al 50% durante las jornadas electorales.

Tales casos ponen en relieve varias limitaciones imputables a la credibilidad de las instituciones electorales, a la brecha de conocimiento existente entre la aplicación de la tecnología y el proceso electoral en sí, y muy en particular, a la ausencia de estándares y/o organismos autorizados para establecer criterios, estudiar y certificar los aspectos relevantes que deben ser revisados y validados en un sistema de votación automatizado para que pueda ser utilizado sin problemas por cualquier ciudadano. Todo esto sin mencionar los escándalos de corrupción en los que se han visto envueltos los gigantes mundiales en la automatización de elecciones.

Ante este panorama de incertidumbre y de desinformación, donde los SAV conocidos hasta el momento no se adhieren suficientemente a los principios de seguridad establecidos para el *software*, y dada la importancia de los sistemas de votación para el funcionamiento de los gobiernos democráticos, la propuesta de Smartmatic Corp., a través de la solución *Smartmatic Automated Election Systems* (SAES) adquiere una relevancia sin precedentes a nivel mundial, por demostrar un profundo conocimiento del origen y la verdadera naturaleza de las fallas y problemas asociados a los

sistemas automatizados de votación, y más específicamente a los sistemas de votación de Registro Electrónico Directo (DRE, por sus siglas en inglés).

SMARTMATIC AUTOMATED ELECTION SYSTEMS (SAES)

Tal y como se demuestra en las posteriores secciones de esta ponencia, todos los detalles de diseño e implementación del SAES parten de un enfoque unificado y completo de las verdaderas amenazas a las que está expuesto un sistema de votación DRE. Un punto común y característico de los sistemas de votación automatizados hasta ahora existentes en el mercado es su extremada propensión a los ataques e intentos de fraude, debido a la relevancia y consecuencias de la información que procesan.

Por ende, la seguridad, transparencia y confiabilidad, tan cruciales en este tipo de sistemas, son implementadas de manera robusta en cada aspecto del SAES y son garantizadas al 100%.

De allí que la clave de éxito del SAES radica en que:

- Cierra consistentemente todas las brechas o puertas de acceso e impide ataques que inutilicen su funcionamiento parcial o totalmente.
- Garantiza que el proceso electoral se implemente de manera correcta e íntegra, incluyendo cualquier particularidad del proceso.
- Arroja resultados que corresponden fidedignamente a la información registrada por los electores.

La aplicación de la tecnología a la automatización de procesos de votación, escrutinio, totalización y adjudicación es de reciente data: al presente se han reportado múltiples situaciones negativas que constituyen una fuente inagotable de experiencia y para evitar repetirlas, han sido estudiadas a fondo y consideradas en su totalidad para garantizar en el SAES: seguridad, transparencia y confiabilidad.

Estos tres indicadores son inequívocos de la robustez de un sistema de votación automatizado, los cuales se ven afectados por la aparición de fallas y desperfectos. A continuación, se presentan las limitaciones más comunes que se han detectado en los SAV en el mundo, a la vez que se

muestra la resolución de los problemas con el sistema SAES para automatización de elecciones.

1. Seguridad

La seguridad es el resultado del conjunto de medidas de precaución implementadas para evitar cualquier causa externa de malfuncionamiento parcial o total del sistema.

En esencia, el funcionamiento de un sistema de votación es relativamente sencillo: sólo debe registrar y totalizar votos. Sin embargo, investigaciones recientes alertan sobre la gran cantidad de fallas presentes en los SAV tipo DRE de ciertos fabricantes en el mercado y las repercusiones que éstas implican.

Las fallas de seguridad en un SAV son numerosas y de diversa naturaleza. Sin embargo, el origen de la mayoría de los problemas de seguridad radica en el paradigma de conceptualización de los SAV, tal y como veremos en las secciones siguientes.

Problema 1. Fallas profusas y generalizadas de seguridad en los SAV

Origen:

- Paradigma erróneo de conceptualización, diseño, uso de metodologías de desarrollo, implementación y pruebas de *software* de votación
- Enfoque de desarrollo de *software* en lugar de desarrollar *software* de seguridad
- Desconocimiento de las verdaderas amenazas a las que se encuentra expuesto el sistema.

Consecuencias:

Sistemas extremadamente vulnerables a cualquier tipo de ataque externo, por lo cual no poseen mecanismos de recuperación adecuados.

Correctivos:

Enfocar el desarrollo de SAV como *software* de seguridad para su diseño e implementación.

A diferencia de cualquier otro tipo de *software*, en el desarrollo de *software* de seguridad se aplican metodologías estrictas y específicas de diseño e implementación: como consecuencia, el modelo de las amenazas de las que debe defenderse el sistema se define claramente desde el principio, lo cual hace posible crear un diseño apropiado que permita contrarrestar cada una de ellas. De allí la implementación de un sistema robusto en su esquema de seguridad, que garantice el resguardo exitoso de todos los puntos vulnerables. Incluso las pruebas de aseguramiento de calidad que se hacen sobre un sistema de seguridad están orientadas a revisar los casos en los que el sistema puede fallar, a diferencia de las pruebas de aseguramiento de calidad aplicadas a *software* común, orientadas generalmente a probar los casos en que funciona el sistema.

Al concebir un SAV con un enfoque de seguridad, varían tanto el diseño como la metodología de desarrollo del sistema, evitando los catastróficos resultados que pusieron en entredicho a ciertos fabricantes en el mercado.

Los ataques más frecuentes a la seguridad de un SAV son los accesos ilegales:

- Al funcionamiento del sistema
- A la información del sistema
- A la configuración del sistema
- A los votos almacenados

Problema 2. Acceso ilegal al funcionamiento del sistema

Origen:

- El control de privilegios de acceso es deficiente
- La información de las claves de acceso no se encuentra encriptada
- Los algoritmos de encriptamiento aplicados sobre las claves de acceso están mal implementados o mal utilizados
- Uso de lenguajes de programación no seguros.

El acceso ilegal al funcionamiento del sistema se refiere específicamente al uso incorrecto de funcionalidades específicas del sistema, mientras el *software* de votación está ejecutándose en tiempo real sobre el hardware

correspondiente. El diseño del sistema considera los usuarios con los que debe interactuar y la modalidad de la interacción. Al no establecerse mecanismos que aseguren la ejecución de las funciones administrativas del sistema por parte de los usuarios correspondientes, se corre el riesgo de que terceros no acreditados burlen el sistema y activen o desactiven procesos específicos que influyan en los resultados de las votaciones.

Cuando el esquema de seguridad de acceso es vulnerable, existe el riesgo de que un elector pueda obtener fácilmente las claves de acceso para realizar funciones administrativas, lo cual implica múltiples consecuencias. Una de ellas es el registro fraudulento de más de un voto por parte de un mismo votante, para cambiar los resultados e inclinarlos a favor de algún partido o candidato en particular. Un votante con las claves de acceso a funciones administrativas también podría provocar el cierre temprano de las votaciones en la máquina, para evitar que aumente la desventaja del candidato que lleve en su haber menos votos. En ambos casos se busca desvirtuar el buen funcionamiento del sistema para realizar operaciones fraudulentas, lo cual podría ser realizado tanto por votantes como por el personal de la mesa directiva de casilla.

Consecuencias:

- Activación arbitraria de las máquinas de votación
- Apertura arbitraria del procedimiento de votación en las máquinas de votación
- Cierre prematuro del procedimiento de votación en las máquinas
- Registro fraudulento de múltiples votos por persona.

Correctivos:

- Utilización de lectores biométricos
- Manejo avanzado de encriptamiento sobre las claves de acceso
- Uso de mecanismos de bloqueo automático de las máquinas al registrar un voto;
- Uso de mecanismos especiales para garantizar los procesos de inicio y término de votaciones en las máquinas
- Control de votos sobre cada máquina.

En el SAES, existe un perfil específico para cada usuario de la máquina de votación, donde los tres principales son: el votante, el personal de mesa y el personal técnico. A cada uno de estos perfiles se les autoriza únicamente las funciones que les corresponden: así, el votante sólo está autorizado para registrar sólo un voto; el personal técnico realiza únicamente operaciones de diagnóstico y mantenimiento sobre la máquina de votación. El personal de la mesa directiva de casilla es el único que puede realizar la apertura y cierre de la votación, y de emitir los documentos oficiales correspondientes.

Cada uno de los perfiles tiene claves de acceso distintas, y cada máquina de votación tiene claves de acceso diferentes para cada perfil, donde las claves de acceso se almacenan de manera encriptada en las memorias de las máquinas utilizando algoritmos de 128 bits o más. Las claves de acceso no están registradas en archivos planos ni en variables estáticas en la máquina.

Todas las máquinas SAES3000 poseen un mecanismo de bloqueo automático para garantizar que cada votante sólo pueda registrar un voto. Se utilizan señales auditivas al finalizar el registro del voto, y se implementan instrucciones que bloquean todos los dispositivos de interacción para imposibilitar el ingreso de información alguna después de registrado el voto. La activación de las máquinas para introducir un voto está a cargo del personal de la mesa directiva de casilla directamente. Además, cada máquina de votación posee el límite de votos que pueden ser ingresados en función de los electores de la circunscripción cubierta por la casilla.

El código fuente está diseñado de forma que ninguna de las variables pueda ser modificada o accedida en tiempo de ejecución. Además, el *software* de la solución está desarrollado utilizando un lenguaje de programación de tipos seguros (Java), para garantizar totalmente la ausencia de fallas por *overflow* o similares.

En el SAES, sólo el personal de la mesa directiva de casilla cuenta con la capacidad de iniciar la votación, al constatar que los contadores se encuentran en cero, a través de las llamadas actas cero o actas de certificación de apertura de la votación.

El proceso de cierre de la votación está implementado en el SAES de tal manera que sólo los funcionarios de la mesa directiva de casilla puede ejecutarlo. Para tal efecto, aplican las restricciones antes mencionadas acerca del manejo de claves de seguridad.

Problema 3. Acceso ilegal a la información de configuración del sistema

Origen:

- Archivos planos con la información de configuración del sistema.

La información de configuración del sistema incide directamente sobre la manera en que los votos son procesados en el sistema. Al modificar esta información, es posible afectar el registro normal de los votos sobre las máquinas, atentando así contra la integridad y veracidad de los resultados. La dirección IP, *login* y *password* de las terminales de votación o la configuración de las boletas electrónicas son un ejemplo de información de configuración que puede ser alterada.

En algunos casos se ha reportado que al acceder a los datos de identificación de red de la máquina de votación, éstos pueden ser modificados o copiados para simular los datos de conexión de la máquina de votación desde una PC cualquiera y transmitir datos adulterados. Este tipo de fraude requiere además que la máquina de votación esté permanentemente en línea para su funcionamiento, o por lo menos durante el tiempo suficiente para que la información pueda ser interceptada durante la transmisión y se realice la sustitución. Si además los archivos de eventos son planos, la información referente a los usuarios y transacciones realizadas por el sistema pueden ser borradas o modificadas.

Una característica común de los SAV previos al SAES, es que el votante no puede ver ni tocar la boleta como tal sino que sólo puede interactuar con una representación de la misma en la pantalla de la máquina. Esto da origen a un tipo de fraude que consiste en alterar la información de configuración de las boletas electrónicas, de modo que el votante marque en la pantalla electrónica una opción específica, pero el voto es sumado a un candidato diferente. Esto sucede cuando la información de las boletas

está almacenada en bases de datos o archivos que carecen de cualquier tipo de protección.

Consecuencias:

- Alteración de los archivos de registro del sistema
- Modificado o borrado de los archivos de registro de eventos
- Modificación de las boletas que aparecen en pantalla
- Extracción de las claves de acceso para funcionalidades administrativas.

Correctivos:

- Encriptamiento de la información de configuración de las boletas electrónicas con algoritmos de 128-bits o superior
- Encriptamiento de la información de configuración del sistema con algoritmos de 128-bits o superior.

Como solución a esta situación todos los archivos del SAES, en los que se almacena la información de las boletas, permanecen encriptados después de su instalación en la máquina tanto en la memoria fija como en el dispositivo de memoria removible. Adicionalmente, es imposible modificar tales archivos mientras el programa se encuentra en tiempo de ejecución.

Tal y como se ha implementado en el SAES, absolutamente ninguna información (claves de acceso, información de configuración del sistema, configuración de las boletas electrónicas) se manipula o transmite en el sistema sin estar debidamente encriptada, evitando así cualquier riesgo que comprometa la seguridad del sistema.

Para reducir el riesgo a un mínimo técnicamente improbable, las máquinas SAES3000 funcionan en modalidad "fuera de línea" a lo largo de toda la votación. Es al cierre oficial de la jornada electoral que se conectan a través de la red pública, utilizando un esquema 'clave pública-clave privada' para comunicarse con los sistemas de totalización a través de un canal seguro sobre la red pública, y con tiempos de transmisión de datos desde las máquinas SAES3000 hasta los sistemas de totalización menores a un minuto. Al reducir el tiempo de conexión se reduce la exposición de

las máquinas de votación y la información a ataques externos a través de la red que pretendan modificar cualquier información de configuración de las máquinas o de los servidores.

Problema 4. Acceso ilegal a los votos

Origen:

- Almacenamiento de los votos en archivos planos
- Almacenamiento secuencial de los votos
- Uso de contadores para totalizar en lugar de almacenar cada voto por separado
- Ausencia de validaciones estrictas en los sistemas de totalización
- Almacenamiento de los votos únicamente sobre dispositivos de memoria externa.

De toda la información que maneja un SAV, la referente a los votos se considera como la más crítica, por lo cual debe recibir todas la protección y restricción de acceso necesarias para garantizar su integridad. Los votos son el blanco de varios tipos de ataques y fraudes, puesto que los resultados de las elecciones tienen enormes repercusiones sobre diferentes factores, especialmente, de tipo políticos.

Ante estas circunstancias, es altamente riesgoso el almacenamiento de los votos en archivos planos, al ser extremadamente propensos a alteraciones o modificaciones por parte de personas externas que eventualmente lograsen franquear las barreras de seguridad del sistema. Mayor es el riesgo cuando los votos deben incorporarse al sistema de totalización, puesto que deben ser transmitidos a través de la red o grabados en una memoria removible para después descargarlos directamente en el sistema de totalización: en ambos casos, el uso de archivos planos incrementa el riesgo de que los datos sean interceptados por personas que conozcan el funcionamiento del sistema y el formato de los archivos, con la intención de alterar los resultados electorales. Si además, el sistema de totalización no realiza validaciones acerca de los votos que recibe e incluye, cualquier ataque que modifique los votos o añada votos falsos tiene altas probabilidades de resultar exitoso.

En lugar de almacenar los votos por separado, en algunos SAV se efectúan únicamente operaciones de incremento de contadores, lo cual impide la revisión de los votos registrados en caso de ser necesario un recuento. Incluso se han reportado casos en los que las variables o contadores de totalización están desprovistas de cualquier tipo de seguridad, siendo vulnerables a los ataques de cualquier persona que pueda acceder al código para modificarlos.

Algunos SAV utilizan archivos de texto para almacenar los votos de manera sucesiva y ordenada; esto atenta directamente contra el secreto del voto ya que la secuencia de los votos podría ser reconstruida (los votos se insertan en el archivo en el mismo orden en que fueron registrados por los electores) y comparada contra los registros de identificación correspondientes, para hacer el enlace entre la identidad del elector y la opción seleccionada.

Consecuencias:

- Alteración de los resultados reales debido al borrado, modificación o adición de votos
- Ruptura del secreto del voto
- Imposibilidad de recuento de votos
- Modificación de los contadores de totalización de votos.

Correctivos:

- Almacenamiento encriptado de cada voto por separado
- Almacenamiento en orden aleatorio de los votos
- Uso de algoritmos de fuentes de alta entropía u otro método confiable para la generación de seriales aleatorios
- Encriptamiento de los contadores.

En el SAES cada voto se almacena por separado en archivos encriptados, y a cada voto se le asocia un identificador digital aleatorio, generado con métodos de última tecnología. De esta manera se garantiza la total seguridad y confidencialidad de los votos.

Cabe destacar que en el SAES cada voto está registrado en siete instancias distintas, las cuales son:

- Voto físico impreso
- Voto almacenado en la memoria removible externa
- Voto almacenado en la memoria fija interna
- Voto sumado en el acta de escrutinio de la mesa de votación
- Voto electrónico transmitido al sistema de totalización
- Voto incluido en las actas de escrutinio electrónicas transmitidas al sistema de totalización
- Voto en las actas de totalización

De este modo se garantiza la integridad de la información, puesto que son siete instancias de registro distintas que, en caso de recuentos, permite comparar nuevamente los votos contabilizados en cada una de las instancias.

Por último, la información de los votos sólo puede ser procesada por las máquinas de votación y los sistemas de totalización, sin ningún tipo de interacción humana. De esta manera, se imposibilita el acceso a los votos, cualquiera que sea la etapa de la jornada de votación.

2. Transparencia

La transparencia del sistema es resultado de su auditabilidad, es decir, de la capacidad otorgada a terceros externos para revisar y certificar que las técnicas de desarrollo del *software* de la votación se hayan utilizado correctamente, que el *software* cumpla con todos los procedimientos establecidos para la votación; además de asegurar que el código fuente del SAV no contenga instrucciones o conjuntos de instrucciones para modificar intencionalmente los resultados a favor de algún candidato o partido específico.

La transparencia también incluye la capacidad que se le da al elector de verificar que su voto ha sido registrado en el sistema acorde a su elección, también denominada "auditoría en caliente" por parte del elector.

Sin duda éste es uno de los aspectos más cuestionados en los SAV conocidos hasta el momento, puesto que la mayoría de las empresas fabri-

cantes de sistemas de votación automatizadas, han apelado al argumento de la privacidad del *software* propietario para evitar la revisión del código fuente por terceros y así mantener oculto el funcionamiento del *software* y los desperfectos del sistema.

Gran parte de la confianza del elector en el Sistema Electoral se basa en la transparencia del sistema utilizado en el procedimiento de la votación, visto éste como garantía de que su opinión será respetada y protegida contra cualquier interés opuesto. Sin embargo, la ausencia de criterios en cuanto a los métodos de auditoría y de herramientas para la revisión del código fuente de un SAV, han repercutido negativamente en la apreciación del público en general respecto a la automatización de los procesos electorales. Y es a través de la auditabilidad del sistema que se puede garantizar plenamente la transparencia del mismo.

La auditabilidad del sistema debe cubrir dos aspectos: los resultados y los procedimientos. En uno se verifica que los resultados concuerdan perfectamente con la información que se ha introducido en el sistema mientras que el otro verifica que las metodologías utilizadas en el diseño e implementación del sistema son correctas y no poseen fallas que alteren de algún modo (accidental o intencionalmente) el funcionamiento del sistema del procedimiento de la votación. A continuación se explican ambas en detalle.

Problema 5. Capacidad nula para comprobar la veracidad de los resultados arrojados por el sistema

Origen:

- Ausencia de voto físico impreso
- Deficientes procedimientos de control del *software* por parte del fabricante
- Falta de conocimiento en la aplicación de tecnología a procedimientos de votación por parte del fabricante.

La crítica más común contra los SAV tipo DRE consiste en la ausencia de boletas o comprobantes físicos, que permitan constatar que los votos electrónicamente registrados en la máquina de votación son los mismos

que los votos contabilizados en las actas de escrutinio emitidas al cierre de la votación. De este modo, la máquina de votación podría almacenar algo distinto sin que el elector pueda constatar el correcto registro de su voto. Igualmente, los funcionarios de mesa directiva de casilla están imposibilitados para constatar y determinar que el voto se haya contabilizado de la manera correcta.

Esta brecha entre el elector y la información procesada por el SAV es blanco de ataques mucho más sofisticados, los cuales provienen en su mayoría de personal con acceso y conocimiento del código fuente, puesto que tienen la capacidad y facilidad de insertar *troyanos* o *malware* sin que esto pueda ser detectado fácilmente al momento de una revisión de *software*.

Consecuencias:

- Desconocimiento por parte del elector de la información que ha sido registrada en la máquina de votación
- Funcionamiento erróneo del sistema que altera los resultados sin ser detectado
- Pérdida de la confianza del elector en el procedimiento de votación.

Correctivos:

- Impresión de voto físico
- Auditorías y pruebas de software para verificación de resultados.

La prueba fehaciente para el elector del correcto funcionamiento de la máquina de votación, es la impresión de un comprobante o voto físico que muestre lo que se ha registrado en la máquina, y que constituya un soporte veraz y certificado de la confiabilidad del sistema.

En este sentido, una ventaja definitiva del SAES en cuanto a la auditabilidad de los resultados, consiste en la impresión del voto físico. En el SAES, el elector señala en la boleta electrónica el o los candidatos de su preferencia (de acuerdo al tipo de elección) y de manera instantánea se despliegan en la pantalla las opciones escogidas, para que el elector verifique así su selección. Cuando el elector registra su voto, la máquina

SAES3000 se bloquea automáticamente e imprime en papel de seguridad las opciones seleccionadas y el número del identificador digital aleatorio correspondiente a ese voto. De este modo, el elector puede corroborar que la máquina registró exactamente las opciones de su selección.

Además, tal y como se indicó en la sección anterior, en el SAES cada voto se almacena de manera simultánea en siete instancias distintas para garantizar la integridad de los votos en el sistema, entre registros físicos y registros electrónicos.

Una de las pruebas más contundente que los organismos certificadores aplican al SAES es la comparación de resultados: éstas consisten en la ejecución de pruebas en donde se ingresan datos específicos asociados a resultados esperados, para luego cotejar los votos físicos impresos contra los votos electrónicos registrados en las máquinas de votación. Gracias a estas pruebas se evidencia la inexistencia de inconsistencias numéricas debido a las siete instancias del voto.

Por último, los procedimientos de implementación del *software* SAES están completamente garantizados por su fabricante, puesto que todo el código fuente se encuentra estructurado y organizado de acuerdo a las más estrictas prácticas de desarrollo de *software* de seguridad, además de estar documentado para garantizar que cualquier organismo que realice la revisión del mismo pueda comprobar en detalle la rectitud de cada función y/o variable utilizada en el sistema.

Problema 6. Capacidad nula para comprobar la rectitud de los procedimientos de desarrollo e implementación del sistema

Origen:

- *Software* propietario bajo secreto del fabricante
- Ausencia de estándares de calidad para sistemas de votación automatizados
- Ausencia de herramientas para realizar auditorías del *software*
- Ausencia de procedimientos de certificación de SAV
- Desconocimiento de la aplicación de tecnología a procesos de votación por parte del fabricante o de las autoridades electorales competentes.

En la mayoría de los casos, no son los organismos electorales quienes desarrollan los SAV sino empresas del mercado que ofrecen soluciones para automatizar elecciones, que luego son rentadas o adquiridas por estos organismos. Por esta razón, gran parte de la confiabilidad del sistema reposa en la integridad de los procedimientos de implementación llevados a cabo durante la construcción del mismo. En este sentido, son los clientes que adquieren los SAV (organismos electorales) los primeros interesados en fijar las normativas y requerimientos que deben cumplir los fabricantes para la adquisición de un SAV. Además, debe existir un acuerdo entre los distintos entes electorales para establecer cuáles son los estándares (a nivel nacional o internacional) que deben seguir los fabricantes y que determinan el nivel de confiabilidad, seguridad y auditabilidad de un SAV.

Otro punto importante es la inexistencia de organismos independientes con la autoridad y el conocimiento técnico, legal, electoral y procedimental necesario para realizar las pruebas y certificaciones que acrediten a los SAV que se ofrecen en el mercado por diversos fabricantes. Cabe decir que en muchos países no existen aún normas legales específicas que delimiten el uso de los SAV.

Hasta el momento, muchos fabricantes han contado con la confidencialidad del código fuente para resguardarse de que terceros externos conozcan el funcionamiento del sistema, sus debilidades y sus fallas no corregidas. Por esta razón, han impedido la interacción abierta con auditores de *software* certificados que no tienen relación directa con el fabricante, por lo cual se mantienen en el desconocimiento público los verdaderos problemas y las implicaciones reales de cada falla.

Consecuencia:

- Funcionamiento erróneo del sistema, accidental o intencional
- Vulnerabilidad ante fraudes y fallas del *software* y/o *hardware*
- Pérdida de la confianza del elector en el procedimiento de votación.

Correctivos:

- Fijación de estándares de seguridad, accesibilidad, confiabilidad, auditabilidad y desempeño para un SAV

- Realización de auditorías de *software* por parte de organismos externos certificados
- Realización de auditorías del sistema por parte de los organismos electorales correspondientes
- Control y uso de versiones certificadas del *software* instalado en las máquinas de votación.

En total conocimiento de las serias implicaciones relacionadas con la transparencia de un SAV, el fabricante del SAES garantiza la utilización de los métodos más avanzados de implementación de *software* de seguridad, recurriendo a sofisticados métodos de encriptamiento, uso correcto y congruente de variables y funciones, documentación y estructura modular del código fuente, entre otros, garantizando que cualquier organismo auditor externo pueda comprobar en detalle la rectitud e integridad del sistema.

Otro aval fundamental es el procedimiento de certificación del SAES por terceros externos, en el cual todos los interesados en auditar el *software* de votación tienen acceso a revisiones detalladas del sistema, y una vez que todos han verificado y comprobado la rectitud del código fuente y el cumplimiento de todas las normativas, se certifica la versión del *software* que luego es instalada en todos los servidores y máquinas de votación. El proceso de arbitrio de tales auditorías puede ser llevado a cabo por el organismo electoral, correspondiente, o por autoridades certificadas que se encarguen de velar por el buen cumplimiento de la normativa y los estándares necesarios para un SAV.

3. Confiabilidad

La confiabilidad es la capacidad que posee el sistema de funcionar en la forma prevista. También está definida como la probabilidad de que el sistema funcione correctamente por un período de tiempo determinado, bajo condiciones determinadas, e incluye la precisión de los resultados que de él se puedan obtener.

Los SAV se consideran sistemas críticos debido a la exactitud y precisión que deben mantener en el registro y procesamiento de la información, durante un intervalo de tiempo muy específico: durante la jornada

electoral. Por esta razón se exige que la confiabilidad de un SAV sea muy cercana al 100% y que todos sus componentes, tanto de *hardware* como de *software*, funcionen de manera óptima.

Problema 7. Fallas generalizadas en el funcionamiento del sistema

Origen:

- Fallas en los tarjetones electrónicos
- Fallas en las máquinas de votación
- Fallas de suministro eléctrico
- Uso de lenguajes de programación ineficientes
- Manejo deficiente del almacenamiento en memorias externas (removibles)
- Fallas en la transmisión de datos desde la máquina de votación hacia los sistemas de totalización
- Máquinas de votación con poca capacidad de procesamiento no actualizables
- Dificultad en la interacción usuario – sistema.

Las fallas de funcionamiento del sistema son atribuibles al *software* de votación y totalización, al *hardware* sobre el cual corren los sistemas (máquinas de votación o servidores), o bien a las redes de datos y/o en la transmisión de los votos o de la información de configuración de las máquinas de votación. Respecto a las fallas de funcionamiento de los SAV conocidas hasta ahora, algunos casos aluden a la imposibilidad de realizar la apertura de la votación sobre las máquinas de votación, privando a una gran cantidad de electores el derecho de ejercer el sufragio.

Consecuencias:

- Sistema parcial o totalmente fuera de línea durante la jornada electoral
- Pérdida parcial o total de votos registrados
- Sistema difícil de manejar para el usuario.

Correctivos:

- Controles estrictos de calidad para cada componente de la máquina de votación
- Pruebas y certificación del funcionamiento del *hardware* del sistema
- Pruebas y certificación del funcionamiento del *software* del sistema
- Funcionamiento de las máquinas de votación con fuentes de poder alternas
- Transmisión encriptada y uso de protocolos de seguridad para el envío de datos a través de la red
- Almacenamiento simultáneo en memorias fijas y removibles; uso del tarjetón electrónico.

Para garantizar la total confiabilidad del SAES, cada componente utilizado en el sistema es sometido a extensas y exhaustivas pruebas de calidad, desempeño, integración y durabilidad. Las máquinas de votación SAES3000 son fabricadas por una de las empresas europeas más reconocidas del mundo en la elaboración de equipos electrónicos, y están diseñadas para facilitar la interacción con el usuario a través de la pantalla sensible al tacto y de los distintos dispositivos que se le pueden incorporar.

Los servidores del SAES operan de manera redundante para garantizar la integridad y disponibilidad de los datos en caso de cualquier contingencia, además de incluir planes de recuperación en caso de catástrofe. En cuanto a las máquinas de votación, las baterías internas garantizan el funcionamiento "fuera de línea" de estas durante toda la jornada electoral y permiten la utilización de baterías externas en casos eventuales de fallas eléctricas serias, sin que esto repercuta sobre la información de los votos o el funcionamiento de las máquinas.

El sistema operativo en cada máquina de votación es Microsoft Windows Embedded, lo cual permite asegurar que el manejo de las memorias externas no pueda ser saboteado o clonado por terceros gracias a la implementación de medidas adicionales de seguridad, tal y como se ha reportado en el caso de conocidos fabricantes en el mercado.

En cuanto a la transmisión de datos a los sistemas de totalización, SAES permite el envío de la información de los votos vía telefónica, vía

transmisión celular o satelital, en enlaces de comunicación menores a un minuto. Los intentos de envíos de datos son realizados por las máquinas hasta que son completados, validados y certificados por los sistemas de totalización para evitar la duplicación de datos.

La configuración y arquitectura de las máquinas SAES3000 es similar a las de una PC, con lo cual se asegura la perdurabilidad en el tiempo del hardware y la actualización y mejoras del mismo, así como de la gran capacidad de procesamiento de la máquina de votación que permite realizar operaciones sofisticadas de encriptamiento de los datos sin influir en el tiempo de interacción del usuario con el sistema.

Otro de los puntos a favor del SAES es la simplicidad de las interfases utilizadas en los sistemas de totalización por los operadores, además del fácil uso de la máquina de votación SAES3000 por parte de los usuarios del sistema de votación. En una pantalla sensible al tacto se despliega, a *full* color y en un tamaño claramente visible, la información que luego es registrada por el elector en la máquina.

Para apoyar la transición de un sistema de votación manual a un SAV tipo DRE, el SAES propone el uso de un dispositivo adicional denominado tarjetón electrónico, el cual es una especie de teclado que imita a las boletas de papel utilizadas comúnmente para marcar el voto, pero compuesta por un conjunto de botones que el elector debe tocar con el dedo en lugar de marcar óvalos con un lápiz. Luego de realizada la selección, el elector verifica en la pantalla que lo tocado en la boleta es lo que ha registrado la máquina. El uso del tarjetón electrónico puede influir favorablemente en la percepción del elector respecto al uso del sistema, al presentarle la información de una manera amigable, intuitiva y muy fácil de usar, de modo que se evite una irrupción abrupta en la idiosincrasia del elector en cuanto al procedimiento de votación.

4. Conclusiones generales

Cuando la tecnología de automatización del voto es correctamente implementada, es posible garantizar la transparencia del sistema y por ende la confianza del elector en el sistema de votación.

La correcta implementación de un sistema automatizado de votación parte de un enfoque de seguridad adecuado que contemple desde la fase de diseño todas las amenazas, peligros y riesgos a los que se encuentra expuesto.

Es de vital importancia la realización de auditorías en los sistemas de votación automatizados antes, durante y después de los eventos electorales, para garantizar ante el organismo electoral y ante todos los actores políticos involucrados la total transparencia del sistema.

Es necesaria la elaboración de estándares para la evaluación del funcionamiento y desempeño de los sistemas automatizados de votación, para garantizar que tales evaluaciones se ejecutan adecuadamente y que el sistema garantice la integridad de todos y cada uno de los votos desde su registro por parte del votante hasta la publicación de resultados.

Escrutinio público del código fuente de Dispositivos Electrónicos de Votación (DEV)

Rodolfo Torres Velázquez,
Instituto Electoral del Distrito Federal (IEDF)

Doctor en Ciencias de la Computación e Ingeniería de Software por la Universidad de Newcastle, Australia. Resultado de su trabajo de investigación son 16 publicaciones internacionales: siete artículos presentados en congresos internacionales, seis reportes de investigación avalados por instituciones de España y Australia, y artículos publicados en revistas especializadas en informática. A partir de febrero de 2003 es titular de la Unidad de Informática del IEDF.

Héctor Campos Estrada
IEDF

Ingeniero en Computación por la Universidad Nacional Autónoma de México. Ha presentado trabajos en 16 conferencias nacionales y dos internacionales. Desde 2002 es director de Desarrollo de Sistemas en la Unidad de Informática del IEDF y participa en el desarrollo del proyecto denominado: "Diseño técnico y desarrollo de la urna electrónica para futuros procesos electorales".

Adolfo Romero Alvario
IEDF

Maestro en Ciencias Computacionales con especialidad en Programación de Sistemas y Tecnologías de Software por el Centro de Investigación en Computación del Instituto Politécnico Nacional. Actualmente es jefe del Departamento de Desarrollo y Mantenimiento de Sistemas V de la Unidad de Informática del IEDF y participa en el desarrollo del proyecto: "Diseño técnico y desarrollo de la urna electrónica para futuros procesos electorales".

RESUMEN

Las democracias actuales deben instrumentar reglas claras y confiables para la competencia electoral, además de garantizar el acceso a la información de manera transparente a todos los ciudadanos. En este artículo se aportan elementos que nos permiten afirmar que el escrutinio público de los programas fuente, que forman parte de la urna electrónica, es un

aspecto fundamental para garantizar la certeza, legalidad, transparencia, confiabilidad e integridad del proceso electoral. Dos aspectos adicionales, e igualmente importantes, que deben tomarse en cuenta son la calidad del *software* y la impresión de un comprobante del sentido del voto. Consideramos que estos tres factores son cruciales para la confiabilidad del proceso electoral con urnas electrónicas.

INTRODUCCIÓN

Con la introducción de elementos informáticos, como lo son los dispositivos electrónicos de votación (DEV), es necesario dar a los ciudadanos, a la autoridad electoral y a los actores políticos los mecanismos e instrumentos de validación que permitan garantizar confiabilidad, certeza e imparcialidad en la realización de la elección.

El escrutinio público de los programas fuente, que forman parte de los DEV o, para nuestro caso, de la urna electrónica, contribuirá a dar confianza de que el código fuente no contiene código malicioso o mal intencionado a favor o en contra de un actor político. Otros dos aspectos igualmente importantes a considerar son: la calidad del *software* y la impresión de un comprobante del voto.

Como parte de la calidad del *software* se encuentra la metodología de desarrollo de sistemas, mediante la cual se desarrolla y estructura la aplicación y los programas que intervienen en el proceso electoral, siguiendo una metodología estándar en el desarrollo de sistemas, lo que redundará en que la comunidad técnica (académicos y técnicos de los actores políticos), así como la ciudadanía podrán revisar la integridad de los programas fuentes. Por último, la impresión de un comprobante del voto permitirá corroborar la correcta operación tanto del *hardware* como del *software* involucrados en los DEV y, realizar conteos físicos y validaciones informáticas con pruebas estructuradas e integrales.

1. Proceso electoral

Actualmente en el proceso de votación es el ciudadano (que ha sido previamente insaculado y capacitado) quien durante la jornada electoral actúa como el funcionario electoral garante de la legalidad del proceso.

En consecuencia, una parte importante de la confiabilidad del proceso descansa en el desempeño de los funcionarios electorales de casilla. Cabe señalar que en caso de una actuación inapropiada, de uno o varios funcionarios de casilla, sólo se vería comprometida la legalidad del proceso en las casillas en las que actuasen estos funcionarios, es decir, el *riesgo* se encuentra distribuido.

En el procedimiento electoral tradicional, el día de la votación el elector recibe boletas impresas en papel seguridad, sobre ellas selecciona el partido político o candidato de su preferencia y, posteriormente, las deposita en una caja transparente llamada "urna". La urna es transparente para que se pueda verificar que ésta se encuentra vacía al inicio de la votación. Al término de la votación se realiza el escrutinio y cómputo de los votos. A partir de ese cómputo se determinan los resultados electorales.

Cuando se utiliza la urna electrónica, ésta reemplaza al funcionario electoral de casilla en cuanto al procedimiento de escrutinio y cómputo; ya que la urna electrónica incluye programas (*software*) encargados de registrar, clasificar y computar los votos emitidos por los electores. Con este esquema, debemos creer que los programas que se ejecutan en ese dispositivo electrónico de votación, están correctamente escritos y por tanto son confiables. Pero existe un aspecto importante a destacar: El mismo programa se ejecuta en todas y cada una de las urnas electrónicas, de tal forma que si el programa no se ha escrito correctamente, la misma falla se presentará en todas las urnas electrónicas; en este caso el *riesgo* se encuentra centralizado. Es por ello que la verificación de los programas que se ejecutan en una urna electrónica resulta fundamental en la confiabilidad del proceso electoral.

A partir de la anotación de algunos aspectos teóricos relacionados con la garantía de que los programas de cómputo son correctos, procederemos a desglosar tres factores que, a nuestro juicio, abonan en la confiabilidad de los programas y del proceso electoral en su conjunto: Calidad del *software*, escrutinio público de los programas fuente, e impresión del sentido del voto del ciudadano.

2. Garantía de corrección de los programas de cómputo

Con el propósito de responder a la pregunta de ¿Hasta dónde es posible garantizar que un programa sea 100% correcto? Conviene tener presente que un programa de cómputo es, o debe ser, la expresión de un algoritmo.[99]

Desde los comienzos del desarrollo de la teoría de la computación se ha demostrado que existe un conjunto de problemas que no tienen, ni tendrán, solución desde el punto de vista computacional; entre ellos destacan que:

- Si un algoritmo es efectivamente un algoritmo; es decir, no existe, ni existirá en el futuro, un mecanismo automático que responda a la pregunta de ¿si un algoritmo es realmente tal?
- Si un algoritmo tiene, o no, un tipo particular de error.
- Si un algoritmo es, o no, correcto; es decir, que cumple con las especificaciones.
- Si un algoritmo tiene, o no, una determinada funcionalidad oculta.

Ello explica por qué los fabricantes de *software* no pueden garantizar que sus productos estén libres de errores y, por tanto, sean 100% confiables.

Para afrontar estos problemas se han desarrollado metodologías de construcción de programas y de pruebas que permiten, hasta cierto punto, atenuar la incertidumbre acerca de la corrección de los programas de cómputo.

Sin embargo, y dada la naturaleza de los procesos electorales, que no admiten dilación, aplazamiento, o márgenes de error "aceptables", se requiere de enfoques complementarios que aseguren un máximo de confiabilidad en los mecanismos de votación automáticos.

[99] Por algoritmo debe entenderse la descripción de una secuencia de instrucciones que concluye en un número finito de pasos.

3. Calidad del *software*

Un aspecto importante que influye en la calidad del *software* son las pruebas. Dentro del proceso de desarrollo de *software* existen diversas etapas. La primera de ellas consiste en la definición de requerimientos. Esta etapa servirá como punto de partida para la definición del conjunto de pruebas a que deberá someterse el *software*. Lo que nos permitirá contar con parámetros objetivos que servirán de referente para determinar lo que debe entenderse por un desempeño correcto del *software*. Aunque, hay que tener presente que la ejecución exitosa del conjunto de pruebas no garantiza la total ausencia de fallas.

El segundo aspecto, es la integridad de los datos, es decir, que los votos de los electores no se deben perder, alterar, comercializar. La privacidad del votante debe garantizarse 100 por ciento.

El tercer aspecto es la integridad del *software*, de manera tal que se asegure que los programas responsables de cada tarea realicen la función prevista.

Pruebas

Una vez concluido el desarrollo de *software*, se debe iniciar la etapa de pruebas integrales para garantizar que los programas encargados del registro de la votación son correctos.

De acuerdo con Deutsch[100] "El desarrollo de sistemas de *software* implica una serie de actividades de producción en las que las posibilidades de que aparezca el fallo humano son enormes. Los errores pueden empezar a darse desde el primer momento del proceso, en el que los objetivos... pueden estar especificados de forma errónea o imperfecta, así como [dentro de] posteriores pasos de diseño y desarrollo.".

De lo anterior se infiere que el *software* de votación debe someterse al mayor número posible de pruebas de diverso tipo. Estas pruebas del *software* son un factor crítico en la calidad del *software* y coadyuvan en la revisión final de las especificaciones, del diseño y de la codificación.

[100] Deutsch, M., *"Verification and Validation", in Software Engineering*, R. Jensen y C. Tonies (eds.), Prentice Hall, 1979, pp. 329-408.

Las pruebas que se realizan para probar un *software* usualmente se realizan en entornos normales. En contraste, las pruebas de un *software* de votación deben llevarse a cabo en condiciones críticas de operación; lo cual es indispensable por la naturaleza de los procesos electorales que no admiten dilación, aplazamientos, ni rangos de error "aceptables".

Adicionalmente, las pruebas solicitadas por los especialistas técnicos de los actores políticos involucrados en la contienda y, aquellas requeridas por instituciones académicas y de investigación de reconocido prestigio, se podrían llevar a cabo con la participación de la autoridad electoral.

Integridad de los datos

Diversos autores sostienen que la integridad de los datos electorales debe verse como un asunto de seguridad nacional, ya que la legitimación de un gobierno democrático depende del proceso electoral mismo. Este argumento es esencial al momento de decidir el nivel de seguridad que requiere un proceso electoral. Así, los votos no pueden ser perdidos, olvidados, alterados, comprados o vendidos, los electores no deben ser coaccionados para emitir su voto, y por último la privacidad del votante se debe garantizar 100%. En resumen, los programas de cómputo que se ejecuten en una urna electrónica deben garantizar la integridad de los datos electorales.

Integridad del *Software*

Según la definición de Roger S. Pressman,[101] la calidad del *software* es: "Concordancia con los requisitos funcionales y de rendimiento explícitamente establecidos, con los estándares de desarrollo explícitamente documentados, y con las características implícitas que se espera de todo *software* desarrollado profesionalmente".

La definición anterior sirve para hacer hincapié en tres puntos importantes:

[101] S. Roger Pressman, *Ingeniería del Software, un enfoque práctico*, cuarta edición, USA, MC Graw-Hill, 1998, pp. 126, 127.

1) Los requisitos de *software* son la base de las medidas de la calidad.

   La garantía de calidad del *software* comprende una gran variedad de tareas asociadas con dos constitutivos diferentes; los ingenieros de *software* que realizan trabajo técnico y un grupo de revisores o garantes de la calidad, encargados de hacer la supervisión, el análisis y los diferentes tipos de pruebas en distintos escenarios.

   Los ingenieros de *software*, quienes realizan el trabajo técnico, tendrán que desarrollar su trabajo con apego a las normas de modelado, documentación, codificación y pruebas internas, perfectamente bien documentadas, para que toda la información quede a disposición del escrutinio público.

2) Los estándares especificados definen criterios de desarrollo que guían la forma en que se aplica la ingeniería de *software*.

   En el marco de los estándares a utilizar, se señala que hay en la industria del *software* una amplia variedad de modelos a seguir y, concretamente, en la industria mexicana, la Secretaría de Economía en coordinación con la Universidad Nacional Autónoma de México desarrollan el "Modelo de Procesos para la Industria del Software" MoProSoft[102] el cual muestra un modelo de desarrollo de *software* que se basa en las mejores prácticas internacionales.

3) Existe un conjunto de requisitos implícitos que a menudo no se señalan. Si el *software* se ajusta a sus requisitos explícitos pero falla en alcanzar los requisitos implícitos, la calidad del *software* queda en entredicho.

4. Escrutinio público de los programas fuente

Diversas instrumentaciones de voto electrónico actualmente en uso, permiten la revisión, en distinto grado, de los programas fuente. Por ejemplo, en el caso de Brasil se "abren" los programas fuente en un entorno estrictamente controlado, durante una semana al escrutinio de partidos políticos

[102] Oktaba, Hanna, *Modelo de Procesos de Software (MoProSoft)*, Secretaría de Economía, México, 2004.

y candidatos; en ese entorno de revisión no se permite la extracción, por ningún medio, de copia alguna de los programas fuente. Mientras que en Venezuela la empresa proveedora posee los derechos del *software* y la revisión del mismo se lleva a cabo por el órgano electoral, previa firma de un acuerdo de confidencialidad y, en Australia, aunque es una empresa privada la que posee los derechos sobre el código fuente, algunos segmentos de éste se encuentran a disposición del público en Internet.

Nuestra propuesta contempla someter permanentemente al escrutinio público los programas fuente de la urna electrónica. Consideramos que ello permitiría a los actores políticos, especialistas y ciudadanos, revisar detalladamente los programas fuente. Lo que posibilitaría contar con la oportunidad de realizar pruebas y, con ello, identificar errores, lo que redundaría en brindar una mayor confiabilidad en el proceso electoral.

La publicación del código fuente permitiría además contar con el tiempo suficiente para la búsqueda de *código malicioso*, *código suspicaz*, identificación de vulnerabilidades, o lógica defectuosa o tendenciosa. Asimismo, posibilitaría verificar que se han utilizado prácticas adecuadas de ingeniería de *software*, por ejemplo que existan suficientes comentarios dentro del código fuente, que los módulos o funciones dentro del código fuente no sean demasiado extensos y que cada uno tenga una entrada y una salida.

Además, la publicación del código fuente no se realizaría necesariamente con la filosofía de GNU/GPL, pues ello implicaría, según lo descrito en http://www.es.gnu.org/Licencias/gples.html, que el *software* electoral pudiera ser modificado y alterado libremente. En todo caso se utilizaría una licencia de GNU modificada en la que se permitiese la revisión pública, pero no así la alteración ni comercialización del *software*, ya que este permanecería como propiedad intelectual del Instituto Electoral del Distrito Federal.

5. Impresión del voto

La imposibilidad material de garantizar en lo general que los programas de cómputo estén libres de errores, conduce a la necesidad de tener un comprobante impreso que permita al elector verificar que su voto

computado a favor del partido o candidato de su preferencia. Así, este medio impreso resulta ser una vía práctica tendente a asegurar la confiabilidad del proceso.

Con este esquema el elector podría verificar, de manera visual, dos aspectos que dan certidumbre al proceso: que en la pantalla se muestre el sentido de su voto, y que el impreso sea fiel reflejo del mismo. Una vez impreso el voto, y posterior a la verificación del elector; el voto se cortaría de manera automática y se depositaría en un contenedor transparente.

Aunado a lo anterior, el comprobante desde su impresión hasta que se deposita en la urna, no tiene contacto alguno con el elector; por dos razones: primero, evitar que el elector pueda llevarse el comprobante, inhibiendo así la posible comercialización del voto y, segundo, que exista una correspondencia entre los datos almacenados internamente de manera electrónica, con los comprobantes que se encuentren en el contenedor.

6. Conclusiones

El procedimiento de votación mediante el uso de DEV o urna electrónica representa un cambio sustancial en la concepción y organización del proceso electoral tal y como está estipulado en la actualidad. Implica, entre otros aspectos, someter al escrutinio de la sociedad, mediante la publicación del código fuente para el registro y cómputo de los votos, la organización del proceso electoral; así como inducir a la población acerca de la convicción de su derecho a conocer a fondo las herramientas tecnológicas con las que se han de realizar los procesos electorales.

Se requiere, en suma, impulsar y consolidar una cultura de transparencia y de acceso a la información técnica, en materia de organización de procesos electorales. A continuación se listan las características generales, que deberá contener un dispositivo electrónico de votación:

- El *software* que se ejecute en la urna electrónica utilizada para registrar la votación, debe ser abierto al escrutinio público.
- Deberá existir un periodo en el que el código fuente sea verificado y certificado (para lo cual se tendrá que realizar un periodo de pruebas

oficiales) por personal técnico de la autoridad electoral, así como por personal técnico de los actores políticos.

- Es necesario definir un estándar para la documentación, los diagramas, las pruebas y el código fuente, para que con base en éste se facilite el intercambio de información y la certificación del *software*.
- La urna electrónica deberá contar con un registro impreso del voto del elector, inhibiendo en todo momento la asociación que pudiese hacerse de la identidad de éste con su voto.

BIBLIOGRAFÍA

IFAI, *Marco teórico metodológico*, México, Instituto Federal de Acceso a la Información Pública, Secretaría de Acuerdos, Dirección General de Estudios y Relaciones Internacionales, 2004.

DEUTSCH, M., *Verification and Validation, in Software Engineering*, R. Jensen y C. Tonies (eds.), Prentice Hall, 1979.

JEFFERSON, David y Aviel D. Rubin, Barbara Simons, David Wagner, *A security analysis of secure electronic registration and voting experiment (serve)*, USA, January, 2004.

OKTABA, Hanna, *Modelo de Procesos de Software (MoProSoft)*, Secretaría de Economía, México, 2004.

PRESSMAN, S. Roger, *Ingeniería del Software, un enfoque práctico*, cuarta edición, USA, MC Graw-Hill, 1998.

La urna electoral mexicana

Ing. Felipe Arturo Ruiz Gutiérrez
Ex presidente y miembro de la Asociación Mexicana de Ingenieros en Comunicaciones Eléctricas y Electrónica (AMICEE)

Ha ejercido la ingeniería de Comunicaciones y Electrónica en el servicio público y privado, y realizado estudios históricos legislativos en las cámaras de Diputados y Senadores. Asimismo fue funcionario distrital del Instituto Federal Electoral.

RESUMEN

La urna electrónica propuesta se adapta a la forma de votar del ciudadano mexicano, de manera que éste simplemente debe introducir la boleta en el dispositivo de votación, el que la marcará en el logotipo del partido o coalición seleccionado por el elector. El ciudadano retirará la boleta y la depositará en la urna correspondiente.

Se describen las características técnicas y operacionales del dispositivo de votación, las que se ajustan a los requerimientos legales que para sufragar fija el *Código Federal de Instituciones y de Procedimientos Electorales* (Cofipe).

INTRODUCCIÓN

La propuesta que aquí se presenta para obtener la automatización de resultados de una elección toma como premisa básica que la forma de votar a la que está acostumbrado el ciudadano mexicano no se altere en lo esencial; para ello, se deben de satisfacer ciertos requerimientos, es decir que:

1. El ciudadano reciba en la casilla, mediante la presentación de su credencial de elector, las boletas para que sufrague marcando en ellas el logotipo del partido político o coalición de sus preferencias.
2. Se mantenga la forma ancestral de votación del elector mexicano, consistente en que éste marque una boleta y la deposite personalmente en la urna respectiva.

3. Una vez que el elector haya sufragado le sea devuelta su credencial de elector y se le aplique la tinta indeleble en su dedo, como señal de que votó.
4. Los resultados de cada una de las elecciones, así como el de votos nulos, se puedan obtener con plena confianza en unos cuantos minutos después del cierre de casilla.
5. No se pueda cometer un fraude cibernético o uno al sufragar por parte del elector.
6. El dispositivo de automatización de resultados tenga autonomía de alimentación eléctrica.
7. Este dispositivo sólo pueda ser activado a voluntad desde la mesa de los funcionarios de casilla.

Este es el esquema general que rige el comportamiento del dispositivo para recibir el sufragio del ciudadano.

Como puede observarse, no se propone una urna con su propio dispositivo de conteo de votación (urna integrada), ya que esto daría lugar a tener tantas urnas integradas como elecciones hubiera, puesto que se necesitaría una para cada elección además de que debería de haber un juego de urnas en cada módulo de votación y esto eleva considerablemente el costo.

Lo que aquí se propone es un Sistema Automático de Cómputo Electoral (SACE), que sirva para marcar la boleta y llevar el conteo de sufragios, dejando al elector que cumpla con el resto de los pasos que implica el votar en una casilla, es decir, no modificar la forma en que el ciudadano mexicano acostumbra votar, de manera que no extrañe el modo en que tradicionalmente lo hecho, además de que siga existiendo una constancia de su voto, es decir, la boleta marcada, que sirve también para dilucidar cualquier aclaración posterior.

Si hubiera un SACE que cumpliera a satisfacción las condicionantes de operación que se dan en esta ponencia, se satisfaría plenamente la razón de emplear la automatización para conocer los resultados electorales, a saber:

- Conocer en la casilla, al término de una elección, prácticamente de inmediato el resultado confiable de dicha elección.
- Poder enviar estos resultados, por vía telefónica, al consejo distrital correspondiente.
- El consejo distrital podría, a su vez, remitir estos resultados al instituto estatal electoral o al federal, según sea el caso, para que éstos concentraran los resultados de los distritos electorales correspondientes.

Todo este proceso se podría hacer máximo en una hora, por lo que a las 19:00 horas se podría tener la información cierta de los resultados de las elecciones terminadas una hora antes, aunque las condiciones horarias de la República obliguen a que estos resultados se den a conocer dos horas después del cierre de casillas en la zona centro. Naturalmente que se seguirían conservando los procedimientos actuales con los que se hace el cómputo electoral, lo que serviría para ratificar los resultados dados por los sistemas automatizados.

1. Automatización de resultados

Como ya se enunció, en nuestro país es indispensable mantener las formas de votación a las que está acostumbrado el ciudadano mexicano, que sirven además para contar con una referencia objetiva de la votación, es decir, que la existencia de la boleta es uno de los requisitos que deben fijarse para aplicar cualquier procedimiento de automatización del cómputo electoral, además de que los partidos políticos deben tener un referente confiable para hacer cualesquier impugnación a una votación efectuada en una casilla o en un distrito electoral.

Aquí es importante señalar que esta ponencia no se refiere a una urna electrónica en el sentido que indica la convocatoria del Instituto Electoral del Distrito Federal, la cual da la idea de una urna automatizada que forma un todo con el recipiente en el cual se colectan las boletas, sino que esta ponencia está dirigida a la creación de un dispositivo que en forma automática marque en la boleta el logotipo por el cual vota un elector, además de llevar la contabilidad del número de votos de cada elección y de otras características que debe reunir dicho dispositivo para satisfacer la

acción ciudadana del sufragio, que aquí se mencionan y que desembocan en que el ciudadano deposita personalmente, como se hace ahora, su boleta en la urna correspondiente; es decir, el concepto de urna que se utiliza en esta ponencia, es el de un recipiente (caja, cajón, arca, etcétera) en el cual se depositan las boletas que ya fueron sufragadas y que no por fuerza deben formar una unidad con el dispositivo que hace la función de recibir las boletas, marcar el voto y computar su número para cada elección, distinguiendo los distintos casos de sufragar que pueden presentarse. Es por esto, que a este dispositivo, que seguramente será electrónico porque sus dispositivos electrónicos y componentes así lo requieren, aquí se le ha llamado SACE.

Una de las condiciones que debe tener la automatización del cómputo electoral es que el cúmulo de formas fraudulentas que se han descrito anteriormente no se puedan hacer o no puedan perpetrarse las que tienen lugar a la hora del sufragio, si se hace el cómputo en forma automática; además de que no se generen nuevos tipos de fraudes al efectuar este tipo de cómputo, a los que podríamos denominar cibernéticos.

Otra condicionante del cómputo automatizado sería que no existiera la posibilidad de error en el número de votos que se adjudicara a cada elección, es decir, que el SACE debe distinguir cada tipo de boleta y asignar el voto de la misma a la elección correspondiente, sin importar que el elector pudiera posteriormente equivocarse al depositar la boleta en la urna. Aquí es importante señalar que si un elector no deposita su boleta en la urna y ya votó en el sistema automático, no habrá posibilidad de que se cumplan las dos premisas antes señaladas, lo cual podría inducir a pensar que el SACE se equivocó, al confrontar sus resultados con los que se obtienen al efectuar el conteo físico de las boletas; es decir, este caso es imposible de detectar por el sistema automatizado de conteo, ya que tiene lugar posteriormente al momento del sufragio. Sin embargo, debe señalarse que este conteo efectuado por el SACE es el correcto. Esto debe tomarse en cuenta al verificar físicamente si no existen boletas de una elección en una urna a la cual no corresponden dichas boletas, o bien, no olvidar la posibilidad de que algunas boletas no hayan sido depositadas por el elector.

También debe tomarse como otra condicionante, el que si una boleta se introduce y el botón, contacto, palanca o mecanismo de sufragio se opera más de una vez, el SACE sólo contará un voto, dado por el primer accionamiento del mecanismo. Puede señalizarse hacia el exterior del módulo de votación, si un elector quiere votar varias veces con una misma boleta. Esta señalización puede ser auditiva, como el sonido de una pequeña chicharra, y visual, mediante el encendido permanente o intermitente de una luz roja. De esta manera los funcionarios de la casilla puede darse cuenta de que el elector que se encuentra en un determinado módulo de votación, quiere hacer trampa.

En el caso de que un elector quisiera hacer trampa utilizando una boleta anteriormente introducida y por lo tanto contada, el SACE deberá detectarla y por lo mismo no efectuar su conteo, ya sea mediante el rechazo de la boleta o mediante la no operación del sistema. En este caso, también se puede efectuar una señalización auditiva y visual fuera del módulo, para que los funcionarios de la casilla se den cuenta de que el citado elector está tratando de hacer un fraude electoral.

El sistema automatizado SACE deberá contar como voto nulo cuando una boleta sea sufragada en más de un emblema de partido o el nombre de un candidato, dependiendo del formato que tenga la boleta. Este voto nulo es equivalente al que se tiene actualmente en el marcaje mediante crayón de las boletas, cuando un elector cruza más de un emblema o cruza toda la boleta.

Actualmente existe en la boleta un espacio para escribir el nombre de un candidato independiente, esto es un absurdo, ya que la ley electoral federal, el Cofipe[103] y las leyes electorales locales señalan que un candidato debe ser propuesto por un partido político; en consecuencia, resulta aberrante que en la boleta se dé la facilidad de votar por alguien que legalmente está inhabilitado para recibir el voto. Es claro que quien vota por un candidato independiente sabe perfectamente que su voto, de

[103] Instituto Federal Electoral, *Código Federal de Instituciones y Procedimientos Electorales y otros ordenamientos electorales*, México, IFE, 1996.

hecho, no tendrá ninguna influencia en el resultado de la elección, por lo tanto, y en forma más realista, el SACE deberá contar con un emblema en blanco para el votante que desee anular concientemente su voto.

En cuanto al cómputo, el SACE deberá contar el total de votos de cada una de las elecciones, así como el total alcanzado por cada uno de los partidos políticos en cada una de dichas elecciones, además del total de votos nulos habidos en cada una de ellas.

Al final de las elecciones, al cierre de la casilla, se cerrará también el SACE por el presidente de casilla, en presencia de los representantes de los partidos políticos, de tal manera que este sistema no pueda recibir ninguna información adicional; es decir, el SACE deberá contar con un candado electrónico que al ser disparado impida que las memorias reciban alguna otra información, actuando ahora el SACE únicamente como reproductor. Con esta condición, el SACE podrá enviar su información a una impresora en la cual se podrá imprimir toda la información contenida en sus memorias.

La información impresa podrá ser transcrita en los formatos de actas y éstas se entregarán a cada representante de los partidos políticos para la firma respectiva. Estos resultados serán los mismos que se den a conocer a los electores en la cartulina que se coloque en el exterior de la casilla.

También el SACE tendrá obligadamente la facilidad de contar con un *modem* (iniciales de modulador-demodulador) para que la información contenida en dicho sistema pueda ser enviada por teléfono a la sede del consejo distrital electoral, lugar en el cual se concentrará la información generada en todas las casillas que se hayan instalado en ese distrito. La información concentrada en el distrito electoral de que se trate se remitirá al Consejo General (edificio central del Instituto Federal Electoral), en el caso de las elecciones federales, de tal modo que en este Consejo se puedan conocer los resultados obtenidos en cada uno de los 300 distritos electorales del país.

En el caso de las elecciones locales, la información obtenida en los distritos electorales locales se recibirá en el consejo local, y se seguirá el mismo procedimiento que se ha señalado para las elecciones federales.

En muchas localidades del interior de la República en donde se instalan casillas, sobre todo en zonas rurales, los cortes de energía eléctrica y las variaciones de voltaje son comunes, situación que también se presenta en zonas urbanas, y esto para cualquier sistema automatizado que seguramente estará alimentado eléctricamente resulta fatal, y por consiguiente para el cómputo de las elecciones. Por lo que es indispensable contar con una forma de alimentación eléctrica que no sea única y forzosamente la red eléctrica pública, además de que la fuente de alimentación tenga una autonomía de cuando menos 12 horas, es decir, poco más del tiempo que jornada electoral, porque puede darse el caso de que exista una falla en la red pública que dure todo este tiempo, lo que no es normal, pero debe preverse para fines de diseño.

Lo conveniente es que la alimentación eléctrica de un SACE, sea hecha por una batería de las comunes de 12 voltios, como las que usan los coches, conectada en flotación y con la capacidad suficiente en amperio-hora para no interrumpir el proceso de cómputo electoral de la casilla, es decir, alimentando permanentemente al SACE, pero siendo a su vez alimentada de la red pública mediante un rectificador adecuado. De esta manera se evita cualquier sistema de *no brake*, que resultaría más costoso.

También es importante considerar lo que sucedería si un SACE, cualquiera que sea su diseño, tuviera una falla en uno de sus circuitos básicos de almacenamiento de la información. Seguramente esto afectaría la función para la cual fue diseñado, que es el de un conteo altamente confiable. La única forma de "asegurar" esta alta confiabilidad es instalando circuitos redundantes en todos aquellos casos en que la práctica de la buena ingeniería lo aconseje, o bien, que se empleen componentes de uso militar, que tienen una elevadísima confiabilidad (son más costosos), es decir, debe considerarse como un requisito de las características del SACE, el que cuente con dispositivos electrónicos redundantes o que esté construido con componentes de aplicación militar en aquellos circuitos que se consideren convenientes.

Con objeto de que el módulo de votación esté controlado, es decir, que no se haga uso arbitrario del mismo, sobre todo en las áreas rurales

en las que se da el control caciquil, es conveniente que en cuanto el presidente de casilla entregue las boletas al elector, el presidente active el SACE que se encuentre en el módulo de votación que haya señalado para sufragar a dicho elector. Esta activación del SACE se deberá de hacer desde la mesa de funcionarios de casilla concretamente por el presidente o en su caso por el secretario, mediante la operación de un interruptor de botón o de palanca. De esta manera, el SACE no consumirá energía mientras no haya un elector en disponibilidad de sufragar, lo que es muy importante para determinar la capacidad mínima en ampere-hora de la batería que se conecte en flotación, lo que trae consigo un menor costo de ésta. También es importante señalar que el presidente de casilla debe desconectar o desactivar el SACE en cuanto el votante haya abandonado el módulo. No se considera necesario que el SACE marque el término de la votación de un elector, lo que se podría hacer, debido a que debe dejarse a cargo de los funcionarios la operación de la casilla y éstos deben estar atentos a lo que suceda en la misma.

Finalmente no debe olvidarse que cada uno de los SACE debe localizarse exactamente en la casilla que le corresponda la cual tendría en su memoria el número de la casilla, la sección distrital, el distrito electoral y la entidad federativa. Estos datos pueden ser cargados por el presidente de casilla en presencia de los representantes de los partidos políticos, antes de la apertura de la casilla, o bien, en la junta distrital, siempre en presencia de los representantes de los partidos políticos ante el consejo distrital y entregárselos al presidente de casilla con el material electoral.

Las funciones que debe realizar el SACE, no se reducen únicamente a las propias de este dispositivo, sino que deben ser complementadas por la propia boleta, esto quiere decir que la automatización del cómputo debe de operar como un conjunto SACE-boleta, lo cual resulta lógico, porque son los dos elementos que intervienen en el proceso de votación y cómputo. Por lo tanto, la boleta debe tener algunos datos que sirvan para que el SACE pueda distinguirla y pueda enrutar el sufragio que se asigne a dicha boleta, a la elección correspondiente. No nada más la información contenida en la boleta puede servir para distinguir el tipo de elección, sino que puede contener otra información para saber si es una boleta

válida o ya fue utilizada, en fin, contener la información útil que sea necesaria para que se cumpla satisfactoriamente la función de cómputo electoral con entera seguridad y exactitud. Esta información puede ser de tipo magnético, óptico o de forma, o de cualquier otro tipo que pueda implementarse en la boleta para que el SACE ejecute todas las funciones para las cuales fue diseñado.

2. Características operacionales

Todas las características del SACE que se han mencionado y que son las que se ajustan a la forma de elección en nuestro país, pueden concretarse en el siguiente resumen:

Características operacionales de un SACE

1) Identificación del SACE.
   a) Entidad federativa
   b) Número de distrito electoral de la entidad federativa
   c) Sección electoral
   d) Número y tipo de casilla (básica o contigua)
2) Distinguir a qué tipo de elección corresponde la boleta válida que se introduzca.
3) Para cada elección, contará el número de veces que se introduce una boleta válida, o sea el total de votos de una elección.
4) El SACE sólo operará si se le introduce una boleta válida, es decir, si la boleta no ha sido introducida con anterioridad.
5) Si se introduce una boleta apócrifa o una que ya haya sido introducida, el SACE operará, con la posibilidad, si se desea, de señalizar al elemento modular con una luz roja y un sonido de chicharra, indicando así que el sufragante quiere hacer trampa.
6) Si se introduce una boleta válida, contará un voto al partido político o coalición cuyo emblema en un botón sea accionado, para que de esta manera compute el total de votos obtenidos por cada uno de los partidos políticos o coaliciones.
7) El SACE sólo contará un voto, si un elector acciona más de una vez un mismo botón sin haber cambiado de boleta.

8) Si un elector acciona más de un botón sin cambiar boleta, el SACE contará un voto nulo.
9) El SACE deberá tener un botón blanco para que quien desee anular su voto pueda hacerlo oprimiéndolo.
10) Al final de las elecciones, al cierre de casilla, se cerrará la operación del SACE, el cual no podrá recibir ninguna información adicional. Desde ese instante, el SACE sólo operará entregando información.
11) La información almacenada en el SACE, podrá operar una impresora y en su caso, imprimir dicha información.
12) La información almacenada en el SACE, podrá ser transmitida a distancia por vía telefónica.
13) El SACE operará con 12 voltios DC., mediante batería conectada en flotación.
14) Algunos circuitos vitales, deberán ser redundantes o ser construidos con componentes de uso militar.
15) El SACE sólo podrá ser activado y desactivado desde la mesa de los funcionarios de casilla.

La Asociación Mexicana de Ingenieros en Comunicaciones Eléctricas y Electrónica (AMICEE), ha diseñado un circuito que teóricamente cumple estas condicionantes. Este circuito no ha sido construido, por lo que no puede darse mayor información sobre su comportamiento real.

3. Conclusiones

1. Las condiciones democrático-electorales que vive actualmente el país, hacen aconsejable seguir utilizando los instrumentos para votar con los que cuenta el ciudadano; es decir: la credencial de elector y la boleta de votación.

2. También es conveniente que el procedimiento de votación vigente en casillas se mantenga, es decir: la entrega de la boleta electoral al ciudadano para que éste la deposite personalmente en la urna respectiva, una vez que haya sufragado.

3. El objetivo esencial de mantener esta forma de votación es que el ciudadano, como ya está acostumbrado, sienta que en efecto votó, al

marcar en la boleta el logotipo de sus preferencias, además de que se le aplique la tinta indeleble en el pulgar. Además, los partidos políticos pueden contar con una constancia objetiva del voto ciudadano, en caso de que exista una impugnación de cualquiera de ellos.

4. El inconveniente del procedimiento actual del cómputo electoral manual es la lentitud al efectuarlo, siendo más significativo en las zonas rurales.

5. Para eliminar el inconveniente antes señalado, es aconsejable efectuar un cómputo automático, el cual debe ser altamente confiable, exacto y cuyos resultados puedan obtenerse inmediatamente al término de una elección.

6. En consecuencia, el dispositivo que realice este conteo, al que he denominado (SACE), debe efectuar las acciones de cómputo que hacen los funcionarios de casilla y los representantes partidistas para asignar el número de votos que obtenga cada partido, así como el de los votos nulos y el total de votos emitidos, además de satisfacer las dos premisas siguientes:

a) El número de votos emitidos en una elección, debe ser igual a los señalados o marcados como "votó" en las listas nominales, y
b) El número de votos emitidos más el número de boletas canceladas, debe ser igual al número de boletas recibidas por el presidente de casilla.

7. Las funciones del SACE para satisfacer los requerimientos señalados en el punto anterior, se han enumerado en el apartado titulado "Características operacionales" del SACE, en el cuerpo de esta ponencia.

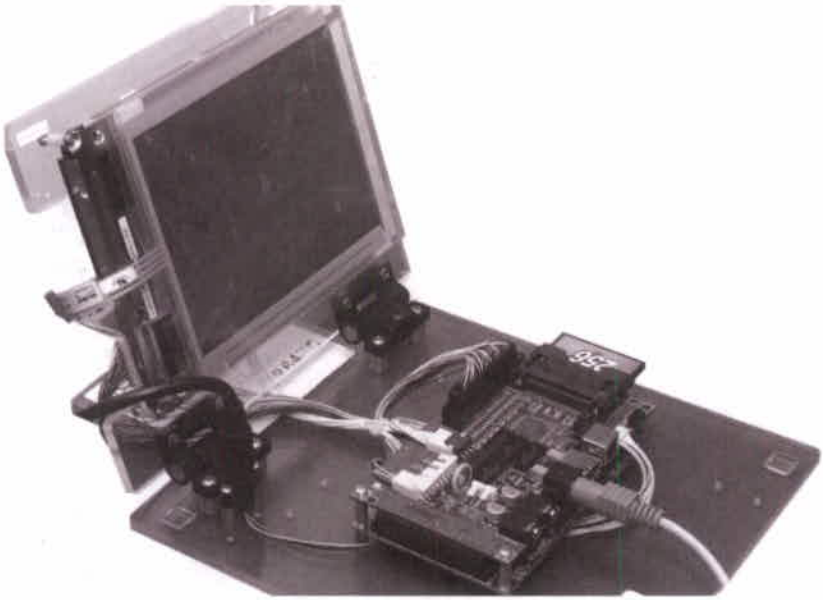
8. Adicionalmente, el costo del SACE debe ser lo suficientemente barato para justificar su uso, considerando que cuando menos deben tenerse dos por casilla y aproximadamente 10% de reserva en el local del consejo distrital para sustituir el equipo que falle. Además, la justificación debe incluir el tiempo de uso del SACE, ya que puede utilizarse para muchas elecciones futuras, tanto federales como locales.

BIBLIOGRAFÍA

CARRANZA, Venustiano, *Ley para Elecciones de Poderes Federales*, México, Diario Oficial de la Federación del 2 de julio de 1918.

INSTITUTO FEDERAL ELECTORAL, *Código Federal de Instituciones y Procedimientos Electorales y otros ordenamientos electorales*, México, IFE, 1996.

Presentación de prototipos y de urnas electrónicas

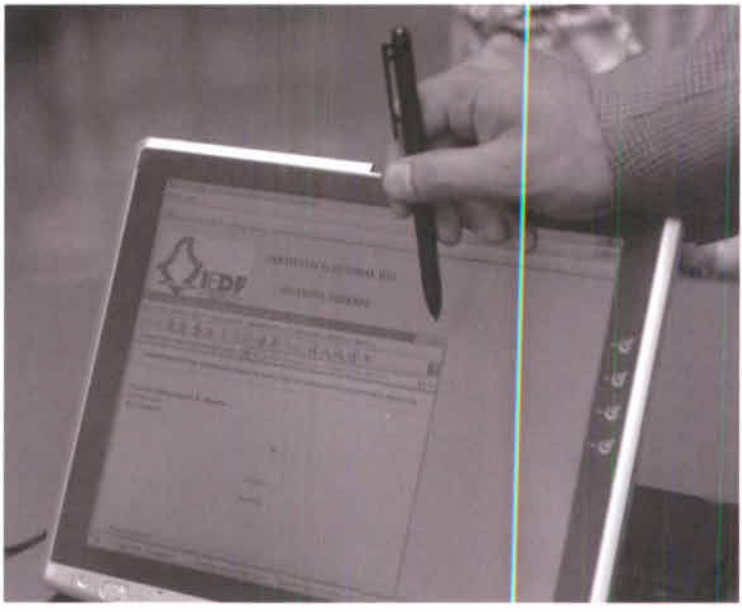


PROTOTIPO

INSTITUTO POLITÉCNICO NACIONAL

(IPN)

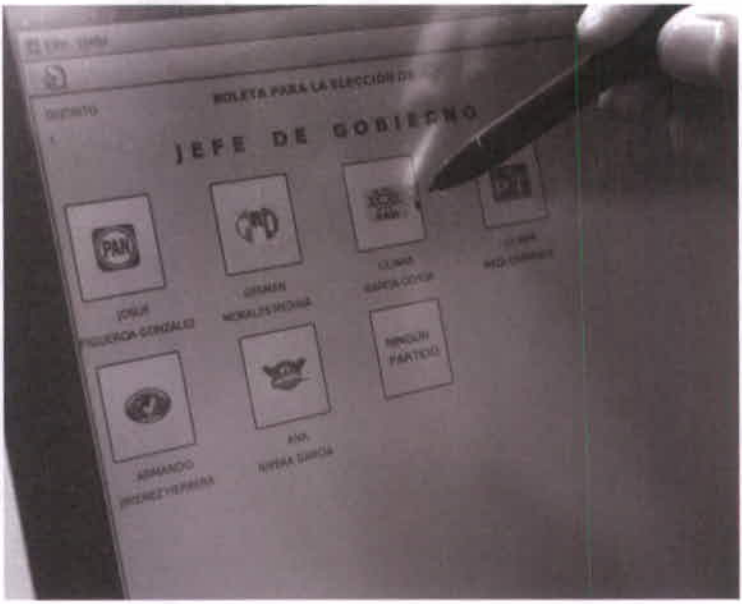
Centro de Investigaciones en Computación



PROTOTIPO

UNIVERSIDAD AUTÓNOMA METROPOLITANA (UAM)

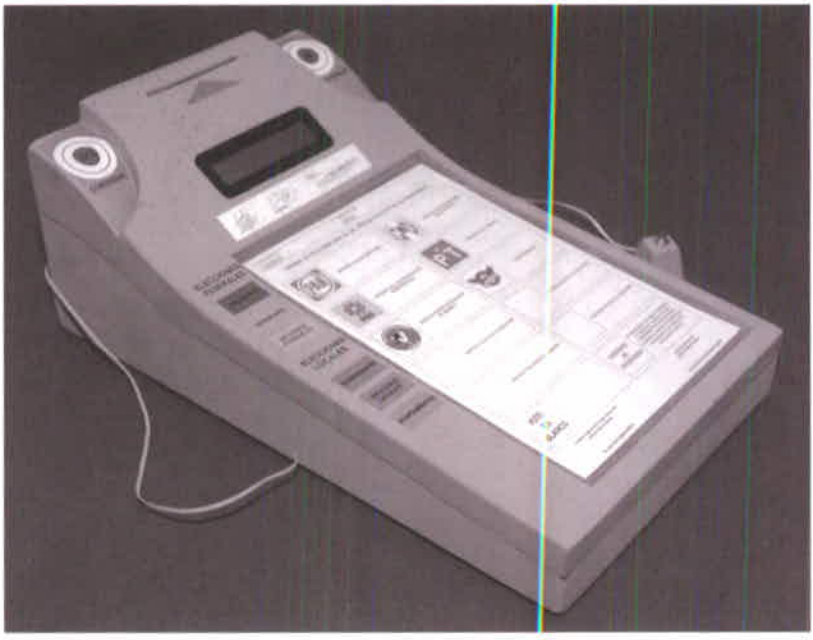
Unidad Azcapotzalco



PROTOTIPO

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY (ITESM)

Campus Ciudad de México



MAQUETA

INSTITUTO FEDERAL ELECTORAL

(IFE)

URNA ELECTRÓNICA

INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE COAHUILA (IEPCC)

URNA ELECTRÓNICA

CONSEJO ESTATAL ELECTORAL
DE SAN LUIS POTOSÍ
(CEESLP)

URNA ELECTRÓNICA
SMARTMATIC

Memoria del Simposio acerca de
las urnas electrónicas para la emisión del voto ciudadano
Se diagramó e imprimió en noviembre de 2005 en los talleres
de GVG, Grupo Gráfico S.A. de C.V., Leandro Valle 14-C,
colonia Centro, 06010, México, D.F.
El tiraje fue de 1 000 ejemplares impresos
en papel bond de 90 gramos y forros en
cartulina cuché de 210 gramos.
Se utilizaron las fuentes tipográficas: Humanst y Optima.
Cuidado de la edición: Unidad de Documentación,
Karina Rosalía Flores Hernández, analista "A".