Gerencia de Capacitación, Investigación y Asistencia Técnica Electoral
Subgerencia de Capacitación e Investigación Electoral

*Área de Investigación Electoral*

# Aspectos tecnológicos del voto electrónico

Luis Panizo Alonso

Serie: Documento de trabajo N.º 17

Panizo Alonso, Luis

*Aspectos tecnológicos del voto electrónico.*--
Lima: ONPE, 2007
60 p.-- (Documento de trabajo; 17)

ELECCIONES / ORGANIZACIÓN DE PROCESOS ELECTORALES /
VOTO ELECTRÓNICO


Jr. Washington 1894 – Lima 1, Perú
Central telefónica: 417-0630
E-mail: <webmaster@onpe.gob.pe>
URL: <www.onpe.gob.pe>

| | |
|---|---|
| Edición: | GCIATE – Área de Investigación Electoral |
| Corrección de estilo: | Odín Del Pozo Omiste |
| Diseño & Diagramación: | Erick Ragas |
| Imagen de carátula: | GIEE (ONPE) |
| Impresión: | ONPE |
| ISBN de la serie: | 9972-695-11-5 |
| ISBN de este número: | 978-9972-695-33-9 |
| Hecho el Depósito Legal en la Biblioteca Nacional del Perú: | 2007-13601 |

Serie: Documento de Trabajo N.° 17
Primera edición
Lima, diciembre de 2007
500 ejemplares

# Índice

# Presentación

La Oficina Nacional de Procesos Electorales (ONPE), como parte integrante del sistema electoral peruano, es responsable de la planificación, organización y ejecución de los procesos electorales, referendos y otras consultas populares. Para el período 2007-2010, la ONPE tiene como una de sus prioridades mejorar la eficiencia de los procesos electorales a través de la progresiva implantación de la votación electrónica con medios electrónicos o cualquier otra modalidad tecnológica, contribuyendo de esta forma al desarrollo y fortalecimiento de la democracia en el Perú.

Dentro de este contexto es que resulta particularmente grato presentar el documento de trabajo que lleva por título: *Aspectos tecnológicos del voto electrónico*. La investigación efectuada por Luis Panizo se ubica dentro de los esfuerzos que la ONPE desarrolla para poner en conocimiento de los especialistas y público en general las investigaciones que se realizan con respecto al tema. El trabajo es especialmente interesante y pertinente, toda vez que expone con claridad el «estado del arte» del uso de las tecnologías de información y comunicaciones en los procesos electorales.

El estudio examina, en primer lugar, el origen, ventajas e inconvenientes, así como las diferentes formas que existen para clasificar el voto electrónico. En segundo término, nos presenta una visión panorámica de las experiencias en el mundo de esta modalidad de sufragio; para, luego de ello, mostrar que en la actualidad las preocupaciones centrales de los investigadores se enfocan alrededor de los temas de uso del Internet para el voto electrónico, sistemas de criptografía para reforzar la seguridad, al igual que en la mejora de los equipos de votación y gestión de los comicios basados en tecnologías de información y comunicaciones. Asimismo, en el análisis se señala la importancia que se debe conceder a los estándares. Finalmente, el autor concluye presentando un conjunto de reflexiones a tener en consideración al momento de poner en marcha sistemas de votación electrónicos.

Con este documento de trabajo, la ONPE continúa con su objetivo de ofrecer a todos los miembros de la sociedad un estudio actual y relevante sobre el voto electrónico. Además, busca incentivar análisis y reflexiones acerca de la aplicación de tecnologías de información y comunicaciones a los procesos electorales, con la finalidad de mejorar la eficiencia de los mismos y fortalecer la democracia en el Perú.

*Lima, noviembre de 2007*

# Abreviaturas usadas

| | |
|---|---|
| AVM | *Automatic Voting Machine* |
| CoE | Consejo de Europa |
| CSFE | Consejo Superior de Franceses en el Extranjero |
| DRE | *Direct recording electronic systems* |
| EAC | *Electoral Assistance Commission* |
| EVM | *Electronic voting machines* |
| HAVA | *Help america vote act* |
| OCR | *Optical character recording* |
| PAD | *Portable application description* |
| PC | *Personal computer* |
| TIC | Tecnologías de la Información y de las Comunicaciones |
| UE | Unión Europea |
| VE | Voto electrónico |
| VVAT | *Voter-verified audit trial* |

# Génesis del voto electrónico

Los intentos de utilizar las tecnologías de la información y de las comunicaciones (TIC) en los diversos aspectos del voto electrónico (VE) pueden parecer recientes, pero no es así. De hecho, una de las primeras aplicaciones de las tecnologías electromecánicas de finales del siglo XIX fue su uso para el ejercicio del VE y del recuento de papeletas posterior. Así, Thomas Alva Edison en 1869 firmó una aplicación de patente (N.º 90646) para un sistema de grabación de voto eléctrico, el cual luego sería utilizado para su primera patente, pues nadie quiso emplearla después. En 1892 Jacob H. Myers diseña la AVM *(automatic voting machine),* que se aplicó en varias ocasiones en el estado de Nueva York (Creelan y Norden 2005). Era un aparato basado en dispositivos de levas que se siguieron utilizando posteriormente en otras máquinas similares (Davis y Boma *machines*).

Con la aparición de los primeros computadores a mediados de la década de 1940 se retomó la posibilidad de utilizar las máquinas para el VE. Así, varios prototipos vieron la luz a mediados del decenio de 1960. Más tarde se han venido utilizando de modo generalizado en todo el mundo para el recuento de votos y el cálculo de resultados

finales. La idea de modernizar los procesos electorales con el empleo de tecnologías basadas en la electrónica proviene de pensadores como Fromm (1955), Fuller (1963), Arterton (1987) y Rheingold (1993). En la actualidad, raro es el país que no haya intentado desarrollar pruebas de voto electrónico con diversos tipos de soluciones y tecnologías.

# ¿Es necesario el voto electrónico? Ventajas e inconvenientes

Muchas son las preguntas sobre la necesidad real de utilizar la tecnología para resolver los procesos electorales. Sus defensores enfatizan las ventajas y minimizan las desventajas. Algunos de dichos aspectos son indiscutibles, pero otros se dan por seguros incluso sin estudios básicos sobre el tema. En la parte positiva destacan tanto la precisión como la rapidez, y en la negativa la falta de seguridad.

Entre los argumentos positivos caben mencionar asuntos como la precisión en la contabilidad de los votos, rapidez en el recuento, incremento de la accesibilidad para discapacitados o por personas con adversidades funcionales, ahorro de papel, flexibilidad, posibilidad de crear una infraestructura permanente para la opinión con voto, mejora de la eficiencia, etc. También se consideran ventajas aspectos más discutibles como por ejemplo el ahorro ecológico, pues las urnas tienen un determinado consumo energético en su fabricación y uso.

Otro punto es que su utilización parece ser más barata que el uso de la urna tradicional; no obstante, hay pocos estudios serios sobre ello. Por poner un caso, en las

últimas elecciones presidenciales con módulos electrónicos celebradas en Venezuela (diciembre de 2006) el costo estimado fue de 200 millones de dólares. Por otro lado, hay análisis comparativos de costos en Estados Unidos entre las urnas basadas en sistemas con exploración óptica *(optical scan systems)* y urnas electrónicas con registro directo o DRE *(direct recording electronic systems)*, pero la variación del precio de compra llega al 900% en función de las características del equipo y su configuración, siendo destacable que en el caso de las DRE se factura el costo de la máquina y el del *software* de forma separada (Hite 2004).

A considerar también está el supuesto aumento de la participación ciudadana en los comicios (Cantijoch 2005; Fernández 2004), aspecto en el cual este trabajo no va a entrar.

En cuanto a los inconvenientes, también son variados y algunos aún no demostrados, como podría ser el costo del sistema electrónico. Lo cierto es que en general la seguridad del proceso de votación está en entredicho y se concluye que la tecnología tiene demasiados riesgos.

Ha sido un error grave de los desarrolladores e investigadores de sistemas y programas considerar que el nivel de seguridad de una votación electrónica es similar al requerido por una entidad financiera (Cox 2004); en ésta, el secreto de la operación puede ser conocido por terceros autorizados y, en cambio, en el voto electrónico el anonimato es parte esencial del mismo, con lo que *nadie* puede tener información sobre el voto salvo en el proceso final de recuento y exclusivamente para la contabilidad. Este tipo de inconvenientes nos obliga a utilizar diversas técnicas de verificación del voto como el VVAT —*voter-verified audit trial*, prueba de auditoría mediante verificación del votante— (Mercuri 2001), lo que complica y ralentiza el uso de las máquinas utilizadas para el voto electrónico. A pesar de todo, hay claras limitaciones en la seguridad de estos equipos si no se toman las medidas oportunas desde el inicio de su diseño (Armen y Morelli 2005; Kohno, Stubblefield y Rubin 2004).

Otro aspecto negativo es la aparente facilidad con la que se podría realizar fraudes con este tipo de dispositivos. En este caso sí hay estudios rigurosos como el de Di Franco y colaboradores (2004) quienes demuestran que con una pequeña manipulación en la copia maestra del *software* de votación es posible producir un fraude electoral a gran escala.

Sin haber resuelto completamente estas críticas, la tendencia actual es el uso de Internet para la emisión del voto electrónico, lo que incrementa enormemente los riesgos en seguridad. En este caso varios autores denuncian el elevado peligro en relación con la seguridad en Internet (virus, troyanos, denegación de servicio distribuida, falta de control por las autoridades electorales de los equipos utilizados por los votantes, etc.), así como por la baja transparencia del procedimiento que incluye la posible pérdida del anonimato (Jefferson 2004; Schryen 2003; Schryen 2004a; Wu y Sankaranarayana 2002). Incluso el propio Vinton Cerf —considerado entre los «padres» de Internet por su aportación al protocolo TCP/IP— cree que una de las debilidades de la Red es su baja seguridad. Sin embargo, no es menos cierto que aparecen ventajas inherentes a la independencia del tiempo y del espacio en la emisión del voto, al probable incremento de la participación al evitar los desplazamientos, a la reducción del coste —a pesar de no existir trabajos rigurosos al respecto—, al decremento de votos nulos, etc.

En cualquier caso, es necesario garantizar una serie de aspectos en el voto electrónico; ello ayudará a que las posibles soluciones sean cuando menos complejas:

1. *Autenticación:* que voten sólo los que estén legitimados para el sufragio.

2. *Unicidad del voto (democrático):* que sólo se vote una vez y no se pueda modificar el resultado de dicha votación.

3. *Anonimato:* que no se pueda relacionar al votante con el voto.

4. *Imposibilidad de coacción:* el elector no deberá en ningún caso demostrar o divulgar qué voto emitió, impidiendo la compra masiva de votos y la presión (coacción) sobre los votantes.

5. *Precisión:* el sistema debe tener la capacidad de registrar los votos correctamente y con seguridad.

6. *Verificación (trazabilidad):* cada votante podrá obtener un recibo del sistema de votación que le garantice que su voto será incluido en el escrutinio final. Existen diversos niveles de verificación, como veremos posteriormente.

7. *Imparcialidad:* todos los votos deberán permanecer en secreto hasta que finalice el período de sufragio. De esta forma se evitará que los resultados parciales afecten a la decisión de los electores que aún no hayan ejercido su derecho al voto.

8. *Auditabilidad:* deberán existir procedimientos para poder verificar que todos y cada uno de los votos se hayan tenido en cuenta en el escrutinio.

9. *Confiabilidad:* los sistemas utilizados deben trabajar de modo seguro siempre, sin que se produzcan pérdida de votos incluso en casos extremos.

10. *Flexibilidad:* los equipos involucrados en el voto electrónico deben ser flexibles con los formatos utilizados (idiomas, posibles elecciones a distintos órganos, diversos tipos de papeletas de sufragio), y ser compatibles con todo tipo de plataformas y tecnologías.

11. *Accesibilidad:* que permita ejercer el voto a personas con adversidad funcional o discapacitados.

12. *Facilidad de uso (usabilidad):* los votantes tienen que ser capaces de votar con unos requisitos mínimos, formación y entrenamiento.

13. *Eficiencia en el costo:* los sistemas tienen que ser asequibles y reutilizables fácilmente.

14. *Certificables:* los sistemas deben poder comprobarse por parte de las autoridades electorales, para que puedan confiar en que cumplen con los criterios establecidos.

15. *Invulnerable:* de forma que impida la manipulación a todos los niveles.

16. *Compatible con la tradición electoral:* que se parezca lo más posible a una urna convencional en su aspecto y uso.

17. *Abierto:* de forma que las autoridades electorales y, si es el caso, el ciudadano en general puedan obtener detalles de su funcionamiento (*hardware* y *software*).

18. *Barato:* que sea competitivo con los costes del voto tradicional.

Sin duda que el cumplimiento de lo anterior está, en mayor o menor grado, en función de los diversos puntos de vista de los elementos involucrados: administración, ciudadanos (electores), empresas y la academia. De esta manera, la administración en general opina que los procesos electorales son complejos, costosos y en algunos casos poco eficientes, además de problemáticos, por lo que intentan utilizar las TIC para su simplificación, mejora y abaratamiento.

Los ciudadanos observan que los métodos utilizados tradicionalmente son arcaicos y en algún caso poco fiables (papeletas perforadas en el estado de Florida en noviembre del año 2000, voto por correo en la mayor parte de los países, etc.), pero no están seguros de que los nuevos procedimientos, empleando la tecnología, cumplan los requisitos imprescindibles. Las empresas ven una oportunidad de negocio ofreciendo máquinas que cumplen con su cometido y muy probablemente estén bien desarrolladas, pero con escaso control por parte del contratante e intentando mantener la solución como una «caja negra» y con la única posibilidad de su verificación desde el exterior (Kohno, Stubblefield y Rubin 2004). La academia ve todo ello como un reto científico y tecnológico, e intenta desarrollar soluciones que minimicen los problemas y garanticen el cumplimiento de los requisitos necesarios.

# Clasificación del voto electrónico

Existe una gran diversidad de formas de sufragar y sistemas involucrados en los procesos de voto electrónico; así pues, su clasificación depende del punto de vista que se adopte. Varios autores la han realizado, pero nosotros preferimos reducir esta clasificación al máximo posible para facilitar su comprensión y flexibilidad. La tipificación más sencilla es la que se produce al dividir los procesos de votación en presenciales y no-presenciales.

Se dice que el proceso de votación es presencial cuando se identifica manualmente al elector, autorizándolo a utilizar una máquina —que en este caso genéricamente se denomina DRE (*direct recording electronic*) o sistema de registro electrónico directo— dispuesta en un lugar específico (colegio electoral). En dicho caso, el proceso de identificación es independiente y no debe de existir la posibilidad de relacionarlo con el voto depositado. De esta manera, toda la información necesaria está in situ; por tanto, se utiliza para ello un equipo específico.

Por el contrario, cuando el voto es ejercido no-presencialmente, es decir, de forma remota, a través de Internet —votación telemática— (Gómez y Carracedo 2004), el

sistema lo hace todo (identificar y enviar el voto) y, probablemente, con independencia del dispositivo (ordenador personal o equipamiento equivalente). Por ende, en este caso, el equipo no es específico (QADAH y TAHA 2007).

Clasificaciones más amplias permiten ver con mayor detalle los procedimientos utilizados y su evolución. *Sistemas tradicionales:* papeletas, tarjetas perforadas, máquinas de palancas o levas. *Modalidad de voto electrónico convencional:* genéricamente urnas electrónicas con OCR (reconocedores ópticos de caracteres), DRE (en general con pantalla táctil y guardado de datos en dispositivos basados en semiconductores) y reconocedores mixtos (híbridos). *Voto remoto o telemático:* en quiosco ubicado en cualquier parte (colegio electoral), no importa el dispositivo con conexión a Internet que se utilice y desde el lugar que sea (voto remoto puro).

Las estadísticas de uso son muy variadas en función del país y el tipo de elecciones, pero dentro de las urnas electrónicas las más utilizadas en los Estados Unidos el año 2004 fueron las ópticas, seguidas de las DRE. En cambio, el voto electrónico puro se ha utilizado en muy pocos países —y menos de forma vinculante, como ha sido el caso de Estonia en marzo de 2007 (BORLAND 2007).

Si nos centramos en los dispositivos electrónicos que podemos utilizar en el VE podemos finalmente clasificarlos, de acuerdo con su uso, en controlado y no-controlado (KRIMMER 2006). En el primer caso podemos tener:

- Terminales de voto electrónico independientes o autónomos *(stand-alone)*
- Mecanismos de voto electrónico conectados a red *(networked)*

Y en el segundo (no-controlado):

- Aparatos para voto electrónico remoto o telemático (PC, móviles, PDA)

Incluso podemos considerar el caso de dispositivos que puedan utilizarse en ambos ambientes, controlados y no-controlados, como los quioscos para voto electrónico conectados a red.

# Estado del arte del voto electrónico en el mundo*

La mayoría de los países en el mundo ha considerado el uso del voto electrónico. De ellos, una buena parte ha realizado pruebas y algunos ya lo utilizan de forma vinculante. En varias repúblicas de Europa se han implementado diversos esquemas con sus respectivas pruebas. En otros lugares —varios Estados de Estados Unidos, en Brasil, seguido de cerca por México—, el empleo del voto electrónico está ampliamente desarrollado. Asimismo, está siendo considerado en buena parte de los países de América Central y del Sur. Además, tenemos a un grupo de antiguos países que formaron la ex Unión Soviética, India y Australia. Vamos a ver con más detalle el estado del arte en dichas naciones.

---

* «Estado del arte» (*State of the art*, expresión tomada del inglés), hace referencia al grado más alto de desarrollo conseguido en un momento determinado sobre cualquier aparato, técnica o campo científico. (N. del E. adaptada de <http://es.wikipedia.org/wiki/Estado_del_arte>.)

*Suiza*

La Confederación Helvética —como sabemos— está fuera de la Unión Europea. Ella es un ejemplo a seguir por el desarrollo en la implantación del voto electrónico. En este país, dividido administrativamente en 23 cantones, se llevan a cabo consultas de forma continua, por lo que era muy utilizado el voto por correo. Posteriormente, y durante varios años, en algunos de los cantones se pusieron en marcha pruebas de voto electrónico empleando diversos métodos. Estudios ulteriores determinaron su uso vinculante, sobre todo después del alto incremento en la participación que se produjo en los referendos de 2003 y 2004 realizados en Anières, Cologny y Carouge (Braun y Brändli 2006).[1] Hoy la mayor parte de los ciudadanos suizos utilizan y confían en el voto electrónico.

*Bélgica*

El reino de Bélgica, integrante de la Unión Europea (ue), fue el pionero del voto electrónico en ese continente. Lo utilizaron en el cantón de Verlaine en 1991, con tarjeta magnética y lápiz óptico. En octubre de 2000, ya el 42% de la población sufragó electrónicamente. En cualquier caso, este país es muy especial debido a que el voto es obligatorio y su sistema electoral muy complejo, por lo que el uso del voto electrónico es valorado positivamente por la administración electoral.

*Holanda*

El reino de los Países Bajos ha llevado a cabo grandes pruebas con estas tecnologías, incluyendo el voto por Internet y a través del teléfono. El mayor ensayo se desarrolló en junio de 2004 para las elecciones al Parlamento Europeo. Hoy en día se puede votar electrónicamente, pero la opinión de los ciudadanos está dividida, sobre todo después de una demostración en directo, por televisión, de cómo se puede modificar una parte del *software* de la máquina y recibir emisiones radioeléctricas a distancia con información de quién está votando (Gonggrijp y Hengeveld 2006). La empresa que fabrica la urna (Nepad) ha garantizado que corregirá los errores. Esta misma máquina, con pequeñas variantes, se está utilizando en pruebas en países de la Unión como

---

[1] Ver *The Geneve E-Voting Project*: *Forum mondial de la société civile*. Génova, 16 de julio de 2002. Disponible en: <http://www.geneve.ch/chancellerie/E-Government/formond_socivile.html> (7/12/07; 13:30).

Alemania y Francia. Sin embargo, en Irlanda se duda de su seguridad después de diversos ensayos.

*Inglaterra*

Este país, que integra el Reino Unido de Gran Bretaña e Irlanda del Norte, como se denomina oficialmente, ha desarrollado pruebas a gran escala en el ámbito municipal desde el año 2000. En junio de 2004 se implementó una prueba de voto electrónico en Londres. El proceso seguido es minucioso y se desarrolla con tiempo, obteniendo de esta forma un avance seguro hacia un escenario de voto electrónico bien diseñado y correctamente planificado,[2] lo cual no significa que por el camino aparezcan problemas como el ocurrido en los comicios municipales celebrados en mayo de 2007 en donde se perdieron una parte de los votos. Un estudio posterior critica la falta de un sistema lo suficientemente riguroso de certificación que asegure que tanto el *hardware* como el *software* que se emplean estén libres de vulnerabilidades.

*Escocia*

Junto con Inglaterra y Gales, integra Gran Bretaña. Escocia constituye un caso similar al anterior. Además dispone de uno de los sistemas electrónicos de participación ciudadana *(e-petición)* para el Parlamento escocés más elaborado, analizado y cuidado de Europa.

*Irlanda*

Integrante de la Unión Europea, desde el año 2000 llevó a cabo un proyecto elaborado cuidadosamente para introducir quioscos de voto electrónico en todos los colegios electorales para las elecciones locales de junio de 2004. Finalmente, y gracias a que el proceso fue totalmente abierto, se emitió un informe por parte de dos destacados científicos que pusieron en duda la fiabilidad del sistema y no se llevó a cabo el proyecto (McGaley y Gibson 2003).[3]

---

[2] Cf. The Electoral Commission. *The shape of the elections to come.* 2003. Disponible en: <www.electoralcommission.gov.uk>; y *The electoral pilots at June 2004 elections.* 2004. Disponible en: <www.electoralcommission.gov.uk>.

[3] Cf. Commission on Electronic Voting. *Secrecy, accuracy and testing of the chosen E.V. System.* 2004. Disponible en: <www.cev.ie>.

*Alemania*

Comenzó sus primeras pruebas de voto electrónico en 1999, pero en ámbitos no políticos. Ha elaborado una documentación precisa sobre los requisitos que deben cumplir los equipos involucrados. Posteriormente, en septiembre de 2005, este país de la Unión Europea utilizó el voto electrónico presencial, para las elecciones parlamentarias de forma vinculante en algunos colegios, con éxito desigual. También se desarrolló un sistema de voto por Internet *(i-vote)* que no ha sido utilizado para elecciones legislativas.

*Austria*

Esta república estableció, en julio de 2003, un plan para el voto electrónico.[4] Desde entonces, se han desarrollado pruebas de voto por Internet, en paralelo con las elecciones presidenciales en abril de 2004, con buenos resultados. En la primavera de 2004 el Ministerio del Interior constituyó un grupo de trabajo sobre voto electrónico.

*Francia*

Ya el año 2003 se empleó Internet para elegir a los representantes para el Consejo Superior de Franceses en el Extranjero (CSFE), pero sin conseguir incrementar la participación ciudadana. En este país de la Unión, también se ha utilizado el voto electrónico en colegios electorales seleccionados, usando la huella dactilar integrada en una tarjeta *(smart card),* para las elecciones al Parlamento Europeo en 2004. En los últimos comicios presidenciales de 2007 se emplearon urnas electrónicas por parte de 1,5 millones de ciudadanos de un total de 44,5 millones. Se registraron problemas sobre todo con los votantes de mayor edad.

*España*

También ha desarrollado pruebas de voto electrónico (Riera y Cervelló 2004), pero todas ellas no vinculantes, pues no lo permite la legislación electoral. En febrero de 2005 se implementó la primera prueba de voto electrónico por Internet, la misma que resultó ser un fracaso técnico y de participación (Panizo 2005).

---

4 Cf. Austrian Computer Society (OCG). *E-voting action plan.* 2003 . Disponible en: <www.e-voting.at>.

*Italia*

De forma muy similar a Francia, este país de la Unión también utilizó el voto electrónico no vinculante y a pequeña escala en colegios electorales.

*Eslovenia y Hungría*

Estas repúblicas de la Unión Europea elaboraron una normativa previa sobre voto electrónico en el año 2003, pero no consiguieron la aprobación de sus respectivos parlamentos.

*Estonia*

Es un país pionero en el uso vinculante y flexible del voto por Internet. Ya en el otoño del año 2005, en esta república de la Unión Europea se realizó una prueba piloto avanzada en unas elecciones locales, utilizando *smart cards* con firma electrónica. Ulteriormente, en los comicios parlamentarios de 2007, 30.275 personas votaron por Internet (3,5% de la población). De todas formas, éste es un caso muy especial y difícil de extrapolar, debido a la alta penetración de Internet en la sociedad y a la posibilidad de utilizar la tarjeta de identificación con clave privada y pública (Maaten 2004; Madise 2006).

*La Unión Europea*

La organización que engloba a 27 Estados europeos desarrolló un proyecto denominado *EU CyberVote Project*[5] durante los años 2002 y 2003. El objetivo fue verificar las garantías de privacidad y seguridad en una votación en línea a través de Internet, utilizando terminales fijos y móviles. El piloto fue implementado por las empresas más reconocidas de telefonía y tecnología, muchos suponen que no podría haber sido de otra forma. Las conclusiones son que el prototipo diseñado *(CyberVote prototype)* funciona en condiciones normales, tanto desde terminales fijos como móviles, como se puso de manifiesto en varias pruebas; pero es imposible garantizar su fiabilidad en votaciones reales y en ambientes no controlados, es decir, allí donde están presentes los grandes riesgos en materia de seguridad en Internet.

---

[5] Consultar: <http://www.eucybervote.org>.

Por otra parte, el Consejo de Europa (CoE) constituyó en noviembre de 2002 un grupo de expertos denominados IP1-S-EE para fijar estándares para el voto electrónico (*e-enable voting).* Luego, se formaron dos subgrupos: uno para los aspectos legales y operacionales, y el otro técnico. Pero se verificaron muchas más dificultades de las inicialmente esperadas. Cada país expresó expectativas diferentes en marcos legales distintos y con niveles de seguridad que la industria no podía en aquel momento satisfacer. Además, la neutralidad tecnológica fue planteada en varias ocasiones en el núcleo de la discusión. El principal avance fue reconocer la necesidad de una cooperación muy estrecha entre los expertos legales y los técnicos. A raíz de estas reuniones se produjo la aparición de unas recomendaciones publicadas en septiembre de 2004, por parte del Consejo de Ministros del Consejo de Europa, denominadas Rec(2004)11.[6] Éstas se desarrollan sobre dos principios generales: el voto electrónico ha de ser tan fiable y seguro como un proceso de votación en el que no se utilice tecnología y, además, debe constituir un canal adicional y opcional de voto.

*Los Estados Unidos de América*

Es el único caso en el mundo en el que, debido a la gran complejidad de su sistema electoral, cada Estado e incluso cada Condado determina la forma y los recursos electorales a utilizar. En las elecciones presidenciales de noviembre de 2000, casi el 70% de los ciudadanos utilizó la vía electrónica para emitir su voto, contando con anticuados mecanismos como la tarjeta perforada, aunque también se empleó el voto con lectura óptica y la máquina electrónica de registro automático (DRE).

En los últimos comicios nacionales de los Estados Unidos, celebrados en el año 2004, la mayor parte de los votantes se valió de sistemas automatizados; 13,7% de los ciudadanos sufragaron con tarjetas perforadas; 14% empleó sistemas similares a la manivela de hace más de 100 años; 34,9% votó en equipos de lectura óptica y 29,3% utilizó para sufragar equipos desarrollados bajo el concepto del Registro Electrónico Directo. El principal inconveniente de estos sistemas es la confianza ciega que se deposita en los expertos que supervisan los procesos y la falta de mecanismos de verificación, lo que pone en tela de juicio su validez. Uno de los fallos más

---

[6] Consultar: <http://www.coe.int/t/e/integrated_projects/democracy/02_activities/02_e-voting/01_recommendation/04E-voting%20Rec%20Spanish%20-Traducci%C3%B3n%20Rec%202004%2011%20Comit%C3%A9%20Mins%20Consejo%20Europa.asp>.

destacables de estos sistemas es el que tuvo lugar en el estado de Florida, donde la falta de normativa y control, unida a una tecnología obsoleta (tarjeta perforada), propició que muchos votantes no pudieran saber con certeza qué opción era la que habían marcado. Otro caso muy relevante fue el de compañía Diabold y más concretamente su sistema AccuVote. El profesor de la Universidad Johns Hopkins, Avi Rubin, analizó el código-fuente y determinó la falta de seguridad en el sistema, accediendo al portal FTP de la empresa.[7] Posteriormente, se fueron sumando más verificaciones negativas hasta el punto de que el Secretario de Estado de California, Kevin Shelly, retiró el certificado a 14.000 de estas máquinas y ordenó una investigación por supuesto fraude de la compañía. Los informes coinciden: «El uso de código fuente propietario, que está oculto y es complejo en sí, hace que sea extremadamente difícil determinar la ausencia de código malicioso en el firmware».[8]

En los Estados Unidos existe, pues, un debate muy enriquecedor sobre el uso de la tecnología en los procesos electorales. Desde finales del año 2006 funciona en la Universidad Johns Hopkins un centro de estudio destinado a incrementar la confianza en las tecnologías del voto electrónico. El proyecto está destinado a abordar las inquietudes del público con respecto al empleo creciente de urnas electrónicas en los comicios locales, estatales y nacionales. Es importante resaltar que ésta no es una propuesta privada. La iniciativa denominada *Accurate* (exacta), que por sus siglas en inglés significa elecciones correctas, funcionales, confiables, auditables y transparentes, recibirá un aporte de 7,5 millones de dólares por parte de la Fundación Nacional para las Ciencias de Estados Unidos.[9]

Con el respaldo de la ley denominada *Help America Vote Act* o Ayuda a América a votar (HAVA, por sus siglas en inglés), promulgada en 2002, los gobiernos municipales y locales de Estados Unidos están debatiendo sobre la conveniencia de aumentar la tecnología en los comicios previstos para el año 2008.

Todo indica que Estados Unidos se desplazó hacia la votación electrónica en las elecciones públicas antes de que la tecnología estuviera lista, y que se hizo sin estudios ni pruebas previas. Básicamente, el proyecto —liderado por Rubin— analizará las

---

7 Consultar: <http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html#rebuttals>.

8 En: <http://www.cs.berkeley.edu/~daw/papers/testimony-house07.pdf>.

9 Consultar: <http://www.verifiedvotingfoundation.org/article.php?id=6289>.

máquinas y la programación de votación electrónica, incluida la criptografía que se utiliza para garantizar que los electores mantengan su privacidad, así como los métodos empleados para comprobar que los ordenadores totalicen con precisión todos los votos legítimos; otros miembros del equipo se encargarán de los aspectos legales y de las políticas públicas que hayan recibido poca atención en la transición a la votación electrónica.

Para intentar disminuir las dudas sobre los sistemas automatizados, los investigadores de la Universidad Johns Hopkins consideran necesario abrir los procesos de prueba de los sistemas a la observación por parte de los ciudadanos y organismos independientes. Para ello se deben establecer procesos permanentes de análisis; facilitar los estudios independientes; ejecutar auditorías aleatorias de las máquinas para comprobar que nadie haya manipulado el *software* utilizado; realizar muestreos en sitios aleatorios y en un número específico de máquinas el día de las elecciones para asegurar que cada sistema registre los votos de manera adecuada; impedir que el código-fuente de los equipos pueda ser modificado; exigir una revisión de las pantallas en todas las máquinas de votación para minimizar la posibilidad de votos ocultos u otras anomalías; y contar con la impresión de un registro físico permanente, independiente del recibo entregado al elector al momento de votar para la verificación de su voto.

Claro que todo esto puede hacer que el proceso automatizado se convierta en más complejo y lento que el tradicional, ya que requerirá la verificación manual sobre el proceso automatizado, es decir, dos procesos en uno. Cabe destacar que el profesor Rubin ha publicado recientemente (2006) un libro titulado *Brave new ballot* en el que literalmente dice: «Imagine por un momento que usted vive en un país donde nadie está seguro de cómo se cuentan los votos y no existen registros fiables para realizar un recuento. Imagine que las máquinas cuentan los votos pero nadie sabe cómo lo hacen. Ahora imagine que alguien descubre que estas máquinas son vulnerables a ataques, pero los organismos responsables no toman las medidas necesarias para hacerlas seguras. Si usted vive en Estados Unidos no necesita imaginárselo. Ésta es la realidad del voto electrónico en este país».[10]

---

[10] Traducción mía. Consultar resumen y presentación del autor en: <http://www.bravenewballot.org/>.

Por último, Estados Unidos tuvo una experiencia de voto remoto en 2004 denominado SERVE[11] que fue desarrollado por el Departamento de Defensa para sufragar desde fuera del país. El sistema esperaba 100.000 votos en una primera fase para llegar a seis millones, con un costo estimado de 24 millones de dólares. Después de un análisis de su seguridad —por parte de David Jefferson y colaboradores (2006), en el que se ponían en entredicho muchos de los aspectos de seguridad del sistema—, el proyecto se detuvo.

*Canadá*

Sigue la estela de los Estados Unidos en esta materia. Aunque a escala federal no se emplea el voto electrónico, sí se hace en los ámbitos municipales y locales en algunas ciudades desde 1990. Carece de estándares pero utiliza los norteamericanos. Cada provincia escoge su tecnología y tiene sus propias normas.

*Venezuela*

Es un caso muy especial, ya que lleva muchos años utilizando, con mayor o menor fortuna, el voto electrónico basado en DRE. Este país tuvo algún inconveniente por el procedimiento de verificación del votante mediante lectura de huella dactilar con una máquina denominada «captahuellas» o «cazahuellas». Se plantearon problemas muy interesantes debido a la sospecha de que se pudieran relacionar las listas de votantes al pasar en un determinado orden y el propio voto emitido en una DRE de la empresa Smartmatic, que se depositaba en orden secuencial. De forma que en las elecciones del año 2005 se retiraron cautelarmente, pero se volvieron a utilizar en diciembre de 2006, argumentando que se había roto la secuencialidad empleando un procedimiento de recolocado seudoaleatorio en grupos de diez.

El despliegue tecnológico en los comicios de este país es uno de los más complejos, pues además de los módulos electorales que emiten un boleto en papel que se introduce en una urna convencional para proceder, en algún caso determinado por sorteo, a su recuento manual (verificación por papel), también se usan las mencionadas máquinas «captahuellas» para comprobar la identidad de los votantes mediante enlaces satelitales que permiten verificar ello en «tiempo real». En cualquier caso el recuento resulta

---

[11] Consultar: <http://servesecurityreport.org/>.

lento y complejo debido al diseño del mismo y a la necesidad de realizar la auditoria manual en alguna de las urnas. El proceso va siendo refinado en las sucesivas ocasiones mediante observaciones externas.[12]

*Brasil*

Aprobó en octubre de 1995 una nueva Ley Electoral en la que se definieron las directrices del voto electrónico con la intención de reducir el fraude electoral y minimizar el tiempo de escrutinio. La votación se lleva a cabo a través de una especie de cajero automático con una pantalla, en la que van apareciendo los candidatos y en la que los votantes pueden realizar su selección oprimiendo un botón. Al concluir la jornada electoral, se bloquea el equipo mediante una clave y se imprimen los resultados, a la vez que se obtiene una copia de los mismos sobre un soporte digital (disquete u otro) que se traslada inmediatamente a un centro de recuento para su tratamiento. La urna electrónica fue el único método de votación en los comicios para elegir Presidente de la República en octubre de 2002 y fue empleada con éxito por 115 millones de votantes.

*Los Estados Unidos Mexicanos*

La definición del uso de las diversas tecnologías para el voto, al igual que otros países, en México depende de los institutos o comisiones electorales de los 31 Estados que integran la Federación. Los Estados de Coahuila de Zaragoza, Distrito Federal y San Luis de Potosí tienen urnas electrónicas que ya han sido utilizadas en algunos procesos electorales. En este caso cabe destacar que los desarrollos son propios y los equipos son totalmente auditables. Éstas, sin duda, son dos ventajas fundamentales que tienen pocos países. Únicamente, si se lograra la colaboración entre los diversos Estados y las universidades se podría mejorar el diseño y minimizar costos.

*Australia*

La Mancomunidad de Australia empezó a utilizar máquinas de voto electrónico desde octubre de 2001 (Boughton 2005). Así, en las elecciones parlamentarias de ese año, las usaron más de 16.000 votantes. Posteriormente (2006), el gobierno del

---

[12] Consultar página de la Unión Europea: Misión de observación electoral Venezuela 2006. Disponible en: <http://www.eueomvenezuela.org>.

Estado de Victoria introdujo en las elecciones estatales una prueba general con voto electrónico. Para este año la Comisión Electoral Australiana ha decidido introducir en 29 localidades el voto electrónico para que puedan utilizarlo 300.000 discapacitados visuales.[13] También se va a desarrollar otra prueba de voto remoto a la que tendrán acceso los militares y personal civil desplazado fuera del país en misiones oficiales. Por lo que sabemos, el proceso es llevado a cabo lentamente y con acierto. Es otro modelo a seguir.

*India*

Es un caso excepcional tanto por el número de electores —668 millones—, como por ser pionera en el uso del voto electrónico (¿alguien ha pensado en hacer papeletas para todos estos ciudadanos, con la multitud de partidos políticos que se presentan?). Ya en el año 2004 se distribuyeron por encima de un millón de EVM *(electronic voting machines)* que suministraron dos empresas del propio país, con un diseño sobrio, un costo de fabricación reducido y de manejo sencillo.

La puesta en marcha del voto electrónico en toda la república se hizo de forma paulatina y comenzó en 1989. De esta forma se fue aprovechando la experiencia para aumentar año tras año el número de máquinas. Éste es un buen ejemplo de cómo hacer las cosas, sobre todo si tenemos en cuenta que el voto tradicional en este caso sería muy complejo, por no decir inviable. Más que nunca tienen sentido las palabras de David L. Dill, que es catedrático de la Universidad de Stanford y presidente fundador de la asociación Verified Votting Foundation. En sus declaraciones asegura que el verdadero propósito de unas elecciones no es que los ganadores asuman que han ganado, sino convencer a los perdedores de que han perdido.

---

13 Consultar: <http://www.aec.gov.au/Voting/e_voting/low_vision.htm>.

14 Consultar: <http://www.rules.senate.gov/hearings/2005/Dill062105.pdf>.

# El trabajo de los investigadores

Desde el año 2004, los esfuerzos de los investigadores para conseguir mejoras en las características de los sistemas de voto electrónico se han incrementado de forma importante en todo el orbe. Basta buscar en las bases de datos de los mejores sitios de investigación del mundo para darse cuenta de ello. En este caso, la información se buscó en IEEE, ACM , Elsevier y E-Voting.cc. Después de filtrada y organizada descubrimos que casi el 25% de los trabajos desde 2004 se centran en conseguir que el uso de Internet para el voto electrónico reúna todas las condiciones básicas enunciadas en el apartado de «Ventajas e inconvenientes».

Ulteriormente, con un 15% cada uno, están los relacionados con los diversos sistemas de criptografía para optimizar la seguridad de los procesos y los que tratan de los problemas de identificación del votante. A continuación, con un 10% cada uno, aparecen las investigaciones sobre la mejora de las DRE y la propia gestión de los procesos electorales basados en tecnología.

Por último, figuran varios tipos de trabajos dispersos como: propuestas para solucionar la coerción y el soborno, procedimientos para análisis del código de las aplicaciones de voto electrónico y diseño de otros procedimientos de voto apoyados en tecnología. Repasemos las principales propuestas.

## MEJORA DEL VOTO POR INTERNET

En general, la mayor parte de los autores proponen procedimientos basados en criptografía; éstos aseguran el anonimato, unicidad del voto y verificabilidad del mismo, pero no solucionan de forma simultánea otro tipo de problemas como el *no authorized proxy*, que es la emisión de un voto de alguien que ha decidido no participar en los comicios (RAY 2002). Otro autor propone una solución para este problema denominándolo SEAS (BAIARDI 2005). No obstante, la propuesta no resuelve la compra de votos ni la trazabilidad de la dirección IP del voto, por lo que proponen votar desde quioscos.

Uno de los problemas más comunes y de más difícil solución es el que proviene del ataque por denegación de servicio, por lo que varios autores concluyen que Internet no es un medio adecuado para el voto electrónico (SCHRYEN 2004b). Otros investigadores dan soluciones más globales para el *i-vote* proponiendo verificación individual para, de esta forma, evitar teóricamente la extorsión y la compra del voto (ACKER 2004); además, le añaden sistemas de intervención y de autoridad electoral, uso de tarjetas criptográficas para identificar al votante garantizando el anonimato del voto. Lo denominan Votescript (GÓMEZ OLIVA 2006).

Otras propuestas reconocen que Internet es de por sí un canal inseguro y para minimizar dicha realidad proponen soluciones novedosas, como el denominado *repeated vote-casting*, es decir, la posibilidad de votar repetidamente y hacerlo sobre diferentes medios (Internet, urna electrónica, móvil...) y que sólo cuente el último de los emitidos. Este procedimiento, que utiliza un sistema doble de cifrado simétrico, intenta evitar la posibilidad de compra y venta de votos; permite, asimismo, aumentar la confianza del votante respecto a la integridad del proceso electoral (SKAGESTEIN 2006).

Quedan desechadas antiguas propuestas que estimaban suficiente el uso de canales seguros tipo SSL, ya que sirven para evitar la intrusión en el mensaje mas son insuficientes para certificar el emisor, el receptor y el propio mensaje. También hay una buena parte

de las soluciones que sólo ofrecen modelos teóricos basados en criptografía, pasando por alto aspectos menos especializados pero de más compleja solución (Benaloh 2006; Delaune 2006; Dini 2002).

Da la impresión de que la mayor parte de los esfuerzos contemplan de forma parcial las posibles soluciones o mejoras, debido probablemente a la complejidad de abordar el asunto globalmente. Por otra parte, se constata que la mayor parte de las propuestas no se apoya en el esfuerzo de otros, con objeto de desarrollar soluciones conjuntas en un tema tan complejo como el voto remoto a través de Internet. Parece que una solución integral aún está lejos.

## Identificación del votante

En este caso, las propuestas están más unificadas y parece que hay un acuerdo tácito de no utilizar los sistemas basados en la biometría (Hof 2004), por los riesgos que ello comporta. Se recomienda el uso de tarjetas de identificación electrónica en clave pública y privada, ya que estos sistemas de claves asimétricas permiten enviar la parte pública por cualquier canal, sea o no seguro. Los mecanismos de anonimato mediante «firma ciega» (Kang e Im 2006), que son complejos en su implementación, tienen el inconveniente de que el usuario no sabe lo que firma, aunque puede obtener un recibo impreso de su voto.

Por tanto, parece que la tendencia más razonable es identificar al votante mediante una tarjeta de identificación (con par de claves, pública y privada) que le permita utilizar cualquier medio, incluido el voto remoto. Un buen estudio a este respecto es el de Kofler (2004) en el que matiza que muchos de los problemas del voto electrónico (secreto, personal y libre) son los mismos que los del voto por correo.

## Criptografía para ocultar el voto

La parte más compleja del voto electrónico está en el núcleo del mismo, es decir, en su esencia de secreto. Por tanto, muchos de los estudios del voto electrónico se refieren al uso de la criptografía desde el mismo momento de votar hasta que se realiza el recuento. Todas las propuestas intentan cumplir, al menos teóricamente, con los requisitos de:

secreto del voto, privacidad, exactitud, integridad del proceso, unicidad del voto —con matices— (VOLKAMER y GRIMM 2006), legitimidad, sistema robusto y verificabilidad universal. Por todo ello, las soluciones son complejas y variadas (WANG y LEUNG 2004). Algunos autores proponen esquemas criptográficos más sencillos basados en agentes *offline* que parecen cubrir todos los aspectos de seguridad con garantías (SANDIKKAYA y ÖRENCIK 2007).

## ESTUDIOS Y PROPUESTAS SOBRE LAS DRE

Son importantes y serias las contribuciones en esta materia que aportan los investigadores, sobre todo de los Estados Unidos. En este caso las soluciones válidas son menos complejas, ya que procesos como el de la identificación y el recuento están desconectados de la red y se realizan aparte. En general, los autores concluyen que las debilidades de los sistemas basados en las DRE no se deben a problemas técnicos, sino más bien al mismo procedimiento de los comicios.

La mayor parte está de acuerdo en las ventajas de la copia impresa del voto, aun teniendo en contra los problemas de usabilidad creados. Este tipo de soluciones son las recomendadas por el movimiento HAVA (Ayuda a América a Votar) en Estados Unidos (FISHER y COLEMAN 2005). También es cierto que hay científicos experimentados que niegan que estos equipos puedan ser utilizados, pues un análisis a fondo del código-fuente deja en entredicho aspectos como el acceso no autorizado, uso inadecuado de los sistemas de cifrado, posibles vulnerabilidades si se conecta a la red y desarrollo de *software* de baja calidad (KOHNO 2003). Sin duda es cierto, pero lo es sobre una máquina en concreto y en un momento determinado. Este tipo de trabajos es muy importante para detectar las deficiencias y corregirlas, y no para anular el resto de los esfuerzos sobre la materia. El análisis del código es realmente complejo, e incluso algunos expertos han llegado a decir que es imposible si se quiere garantizar su fiabilidad y precisión al 100% (RUBIN 2006). Pero está claro que en la tecnología no hay nada 100% fiable.

## GESTIÓN DE LOS PROCESOS ELECTORALES

Los informes sobre investigación del voto electrónico dejan claro que la seguridad de éste depende de dos aspectos bien diferenciados: la parte técnica y el procedimiento.

En general, el segundo está más descuidado, pues se «heredó» de los procesos electorales clásicos, por lo que algunos detalles son insuficientes para garantizar la seguridad en el voto electrónico. Por ejemplo, hay ausencia de suficientes procedimientos de control sobre los suministradores del equipamiento, al igual que de los encargados de la supervisión; por ello, es necesaria la mejora de los procesos en sí, junto con la formación del votante y de los agentes implicados, y por último definir con claridad el papel de cada agente en el proceso electoral (Xenakis 2006; Xenakis y Macintosh 2004).

Lambridoudakis y colaboradores (2003) concluyen que los esquemas tradicionales de autenticación y autorización no cubren completamente los requisitos de seguridad del voto electrónico, por lo que es necesario ampliar estos modelos de autenticación y autorización, de forma que regulen las acciones permitidas sobre el sistema. Para ello será necesario definir claramente los casos de uso, roles y permisos de cada participante en el proceso.

## Otras propuestas

En otro conjunto de papeles menos habituales aparece una serie de propuestas muy importantes para el desarrollo adecuado del voto electrónico.

Una de ellas, es la posibilidad de utilizar máquinas con «código abierto» *(open source)* y de esta forma facilitar la comprobación del código por terceros, lo cual mejoraría la verificación del sistema en general. Esto está siendo planteado por diversos países, evitando así el efecto «caja negra» con el que las empresas entregan las urnas electrónicas. Dentro de esta posición hay varios desarrolladores que han propuesto soluciones «abiertas» que merece la pena estudiar (Keller 2005).

Por último, un aspecto que cada día está adquiriendo mayor relevancia y atención es el de la accesibilidad a la máquina, entendiendo ésta como las facilidades dadas al colectivo de ciudadanos con alguna diversidad funcional o discapacidad (ceguera, visión deficiente, dificultades motoras, etc.). Dichas facilidades constituyeron, también, una de las recomendaciones del HAVA a los desarrolladores de máquinas DRE y está siendo tomada en consideración en la mayor parte de los países (Hernson 2006). Éste es uno de los aspectos en que el voto electrónico tiene claras ventajas sobre el voto tradicional.

# La importancia de los estándares

Aparte de las recomendaciones, los estándares son de una importancia vital para organizar el uso adecuado y normalizado del voto electrónico en todo el mundo. Lo que ocurre es que difícilmente se puede recomendar, y mucho menos fijar, unos estándares si previamente no se tiene experiencia suficiente, de ahí la importancia de las pruebas y de sus respectivos análisis. Intentar fijar unos estándares a cumplir, antes de haber experimentado o bien utilizando la experiencia de los demás, puede ser un desastre en cualquier tipo de desarrollo o innovación.

Como ya hemos comentado anteriormente, la Comisión de Ministros del Consejo de Europa presentó en septiembre de 2004 unas *recomendaciones* para el voto electrónico. Nadie duda del trabajo desarrollado y de la importancia que éstas tienen, sobre todo en una agrupación de países tan compleja como la Unión Europea. Esto se hizo después de que varios países desarrollaran pruebas a todos los niveles y se llevaran a cabo estudios sobre el tema. A pesar de ello, las recomendaciones realizadas por un grupo de expertos han sido criticadas debido a la pobre expresión de sus contenidos y la necesidad de mejorar la forma en que se expresan. Es probable que una simple

reestructuración sea un buen comienzo para el proceso de mejora (McGaley y Gibson 2005). No obstante, como cualquier otro tipo de recomendación, ésta debe ser optimizada obteniendo información sobre su aplicación en las pruebas de los diversos países. Sin duda es un punto de partida.

Por otro lado, es significativo destacar el caso de los Estados Unidos de América, en el que la Comisión Electoral Federal y posteriormente la EAC (Comisión de ayuda a las elecciones) determinaron unos estándares que no expresaban un conjunto coherente de requisitos para los sistemas de voto electrónico. Por esta razón, las certificaciones que se han obtenido bajo dicho estándar han sido defectuosas. «Sin un modelo de los riesgos y del sistema, los estándares de votación no pueden asegurar la integridad ni la exactitud del proceso de votación», concluye un trabajo de Earl Barr y colaboradores (2007). La moraleja de esta opinión se apoya en que nadie puede verificar que un sistema no tiene defectos, incluso si todo el código-fuente de la aplicación de voto está disponible. Esta es la misma opinión que la expresada por Avin Rubin y su equipo (2006): Es cierto que es bueno valerse de la duda metódica en cualquier proceso, y más en éste; pero no es menos cierto que si se emplean herramientas y procesos de diseño del *software* involucrado en un proceso electoral de forma correcta, el resultado no tiene por qué ser defectuoso. Por otra parte, como decía David Hume: «Afirmaciones extraordinarias requieren evidencias extraordinarias».

De esta forma podemos estar de acuerdo con los que concluyen que el sistema de voto perfecto no existe, como tampoco existe en ninguna otra aplicación de la tecnología. En cualquier caso, concordamos en que es imprescindible volver a escribir los estándares pensando en los riesgos; ello en colaboración con los fabricantes, la administración, los expertos en ordenadores, así como con los ciudadanos, y de esta forma delimitar los riesgos contra los que sería necesario protegernos. Es necesario ir más allá del camino que se ha utilizado hasta ahora para abordar el diseño de los sistemas de voto electrónico y utilizar técnicas de alta precisión para garantizar que éstos cumplan con las garantías necesarias.

La definición de los estándares en el voto electrónico es uno de los temas más complejos y una asignatura pendiente en todo el mundo.

# Intereses comerciales en el voto electrónico

En la mayoría de los países que utilizan el voto electrónico han estado presentes —de una u otra forma— las empresas que desarrollan, fabrican o venden servicios relacionados con esta tecnología. En ningún caso vamos a valorar sus desarrollos o su trabajo, que sin duda ha sido esencial para el aumento de las experiencias en todo el mundo, pero creemos que hay también otras opciones que no tienen por qué ser incompatibles.

En algunos países, por ejemplo Estados Unidos, los proyectos e investigaciones de alta tecnología —verbigracia los centros de excelencia en materia de seguridad interna *(Homeland security)* e incluso en otros ámbitos menos críticos—, se llevan a cabo en las universidades de primera línea en colaboración con el gobierno. Esta unión entre universidades, centros de investigación y gobierno puede dar resultados espectaculares en el avance de las técnicas de voto electrónico.

Otro caso sería dejar a las empresas su comercialización y distribución. De esta manera el diseño no estaría determinado por parámetros comerciales y podría estar más abierto a la revisión e inspección de terceros, es decir, se le dotaría de transparencia.

Tenemos que evitar los conflictos entre lo comercial y lo democrático. Los problemas de los secretos de empresa, patentes, derechos adquiridos, etc., no deben afectar a la democracia. Como concluye Margaret McGaley: «[...] negocios hay muchos, pero democracia sólo una» (MCGALEY y MCCARTHY 2004).

# Otras posibilidades del voto electrónico

Es fácil imaginar un escenario en el que las infraestructuras desplegadas para el voto electrónico remoto se conviertan en permanentes, en una especie de «infraestructuras estratégicas» para conocer la opinión de los ciudadanos de forma continua. Es evidente que ello cambiaría muchos aspectos políticos y sociales que están fuera del ámbito de este trabajo, pero sería una forma de rentabilizar socialmente el costo de estas infraestructuras tecnológicas.

Por otra parte, el voto electrónico también es utilizado hoy en día con otras finalidades diferentes a la del voto legislativo, en entornos como el empresarial, financiero, asociativo, universitario, organizativo, etc. Una de las principales ventajas es que los requisitos necesarios no son, en principio, tan elevados como en el primer ámbito, por razones obvias de mantenimiento de los principios democráticos —aspecto crítico sin duda (Rüdiger 2006).

# Conclusiones

Es fácil apreciar la falta de sinergia a la hora de desarrollar sistemas de voto apoyados en la tecnología. Una de las consecuencias es la diversidad de soluciones presentes en el mercado, no sólo en el plano tecnológico sino también en el de los procedimientos de gestión de los comicios.

Por ello, es importante realizar un análisis comparativo de las experiencias obtenidas en:

- Proyectos piloto privados.
- Países que ya han introducido el voto electrónico.
- Países con administraciones electorales con pruebas avanzadas.
- Trabajos de investigación de las diversas Universidades y centros de desarrollo.
- Empresas del sector.

Los pasos recomendables para implementar las técnicas de votación electrónica deberían ser:

- Aclarar que el voto electrónico es un medio más y, por tanto, opcional.
- En las primeras fases del paso al voto electrónico conviene mantener la presencia del formato en papel.
- Comenzar con grupos identificados, que por alguna razón no participan habitualmente (personas con diversidades funcionales o con problemas de desplazamiento, etc.).
- Utilizar sistemas con un diseño sencillo, el cual permita su uso por parte de cualquiera, con un mínimo de entrenamiento
- Dar este entrenamiento a usuarios y gestores.
- Ir paso a paso analizando las fortalezas y debilidades del sistema.

Asimismo, es muy recomendable poner en marcha reuniones, foros, mesas de trabajo entre estados y naciones con objeto de intercambiar información y experiencias que ayuden en el desarrollo adecuado del voto electrónico.

Todo desarrollo en esta materia debe de ser considerado en el contexto que está situado y tener presentes las cuatro dimensiones: legal, política, social y tecnológica. También hay que considerar desde el comienzo el tamaño del proyecto que se pretende implementar.

Es necesario desarrollar un esfuerzo importante por partes de los investigadores, apoyados por sus gobiernos, en realizar estudios comparativos —serios y reales— entre la seguridad de los sistemas tradicionales de voto y los basados en la tecnología, con el fin de fijar el grado de seguridad *aceptable* dentro de criterios democráticos. Hay que tener en cuenta que otros canales de participación, como el voto por correo, tampoco son fiables; pero consideramos más esencial facilitar el acceso a la urna, que los criterios extremos de seguridad que se intentan imponer al voto electrónico y que no existen en otros canales.

En los sistemas de voto tradicional se producen pequeños errores de forma continuada, y el uso de la tecnología puede incrementarlos. Para evitarlo conviene avanzar lentamente y en una primera etapa utilizar técnicas de verificación por parte del votante, como los votos en papel. La tecnología bien usada y desarrollada puede convertirse en un aliado poderoso para reducir los riesgos.

Intentar convencer a la gente de que las máquinas son seguras, no es la mejor forma de introducir el voto electrónico. Es preferible hacer todo el proceso «transparente» desde el comienzo y asegurarse de dotar a las urnas de mecanismos de recuento fiables, rápidos, claros y verificables. Por ello es imprescindible utilizar sistemas que permitan auditorias mediante verificación por parte del votante y que éstas reúnan condiciones de accesibilidad.

Una de las facetas más descuidadas del diseño es la usabilidad y es básica para evitar el voto nulo. Como este tipo de soluciones de voto se apoyan en computadores, para conseguir un desarrollo con éxito de los estándares tenemos que contar necesariamente con los tecnólogos, científicos, ingenieros y matemáticos.

Facilita enormemente el voto en urna electrónica y el voto por Internet, el uso de tarjetas de identificación del votante con parámetros biométricos y soporte para claves asimétricas.

No obstante, hay que tener presente que los mayores expertos en tecnología reconocen que ésta tiene dificultades y limitaciones en campos como la privacidad, seguridad y libertad. Después de treinta años de mejoras en la criptografía, algunos de los investigadores están cambiando de punto de vista y dicen que hay que reconocer la realidad de las «estructuras sociales» en contra del ideal de la verdad única de la física y las matemáticas.

Conviene dejar claros los riesgos en la seguridad de la votación electrónica, sin caer en extremos. Es muy aconsejable utilizar «código-fuente abierto» en los desarrollos y máquinas «transparentes» para facilitar las inspecciones y certificaciones. Se desaconseja el empleo de equipos con estructura de «caja negra».

Con la experiencia adquirida, es necesario abordar el desarrollo de estándares serios que permitan certificaciones fiables. De las experiencias mundiales podemos sacar varias conclusiones:

- No hay tendencias únicas en el voto electrónico, incluso en los países con más experiencia.
- Los países que han intentado implementar sistemas a gran escala, sin debate previo ni transparencia suficiente, se han encontrado con la oposición de varios sectores.

- En este tema se producen cambios de opinión de forma continua, lo que demuestra que no ha sido introducido correctamente.
- En muchos países no se han resuelto algunos de los aspectos del voto electrónico (legal, tecnológico, social, político) debido a que no se han explicado claramente las ventajas y el interés público.
- Los mejores desarrollos se han obtenido gracias a una estrecha colaboración y entendimiento mutuo entre los expertos tecnológicos y los jurídicos, para posteriormente incluir a los legisladores, políticos y público en general.

No olvidemos, finalmente, que *todo es cuestión de confianza* (¿no confiamos acaso en los medios de pago electrónicos?).

# Fuentes de información

## Bibliografía


Acker, B. Van

2004 «Remote e-Voting and Coercion: a Risk-Assessment Model and Solutions». En: Krimmer (ed.). *Proceedings: Electronic Voting in Europe,* pp. 53-62. Disponible en: <http://www.e-voting.cc/static/evoting/files/vanacker_p53-62.pdf> (7/12/07; 18:13).

Alvarez, R. Michael y Hall , T. E.

2004 *Point, click and vote. The future of the Internet voting.* Washington, D.C.: The Brookings Institution Press.

Armen, C. y R. Morelli

2005 «E-voting and computer science: Teaching About the Risks of Electronic Voting Technology». *Proceedings of the Tenth Annual Conference on Innovation and Technology in Computer Science Education,* pp. 227-231.

ARTERTON, C.
1987 *Teledemocracy: can technology protect democracy?* Newbury Park, California: SAGE publications.

BAIARDI, F. et ál.
2005 «SEAS, a secure e-voting protocol: design and implementation». *Computers and Security,* vol. 24, n.º 1, pp. 642-652.

BARR E. et ál.
2007 *Fixing Federal E-voting standards*. Nueva York: Comunicación de la Association for Computing Machinery (ACM)

BENALOH, J.
2006 *Simple verifiable elections*. Microsoft Research. Disponible en: <http://www.usenix.org/events/evt06/tech/full_papers/benaloh/benaloh.pdf> (7/12/07; 18:24).

BENKLER, YOCHAI
2006 «Political Freedom Part 2: Emergence of the Networked Public Sphere». En BENKLER, Yochai. *The Wealth of Networks. How Social Production Transforms Markets and Freedom,* Yale University Press. Disponible en:<http://habitat.igc.org/wealth-of-networks/ch-07.htm> (13/12/07; 18:33).

BORLAND, J.
2007 *Online voting clicks in Estonia,* marzo. Disponible en: <http://www.wired.com/politics/security/news/2007/03/72846> (7/12/07; 13:40).

BOUGHTON, C.
2005 *Maintaining democratic values in e-voting with eVACS*. Software Improvements.

BRAUN, N. , D. BRÄNDLI
2006 «Swiss e-voting pilot proyects: evaluation, situation analysis and how to proceed». Disponible en: <http://www.e-voting.cc/static/evoting/files/Swiss_Experiences.pdf> (7/12/07; 13:45).

Cantijoch, M.
2005 «El voto electrónico ¿un temor justificado?» *Revista Textos de la Cibersociedad* n.º 7. Disponible en: <http://www.cibersociedad.net/textos/articulo.php?art=72> (7/12/07; 12:36).

Cox, C. y A. Rubin
2004 *Is the U.S. ready for electronic voting?,* 20/9/04. Nueva York: Times Upfront.

Creelan, J. y L. Norden
2005 *The requirements of New York University School of Law,* noviembre. Disponible en: <www.wheresthepaper.org/brennanctr11_16fullface.htm> (7/11/05).

Delaune, S. et ál.
2006 *Coercion-resistance and receipt-freeness in electronic voting.* ieee. Disponible en: <http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-csfw06.pdf> (7/12/07; 18:26).

Di Franco, et ál.
2004 *Small vote manipulations can swing elections.* Octubre. Nueva York: acm.

Dini, G.
2002 «Increasing security and availability of an Internet voting system». *Computers and Communications.* Proceedings of the Seventh International Symposium on Computers and Communications (iscc'02), pp. 347-354.

Fernández, I. D.
2003 «El voto electrónico». *Otrosí. Revista del Ilustre Colegio de Abogados de Madrid, n.º 62, pp. 46-51*

Fisher, E. y K. Coleman
2005 *The direct electronic voting machine (dre) – Controversy: facs and Misperceptions.* crs Report for Congress Disponible en: <http://fpc.state.gov/documents/organization/60725.pdf> (7/12/07; 20:01).

Fromm, E.
1955 *The sance Society.* Nueva York: Rinhart.

FULLER, B. R.
1963 *No more secondhand God.* Illinois: Southern Illinois University Press.

GÓMEZ, A. y J. CARRACEDO
2004 «Del voto electrónico al voto telemático». *Boletín Red-Iris,* pp. 66-67.

GÓMEZ OLIVA, A. et ál.
2006 «Contributions to tradicional electronic voting systems in order to reinforce citizen confidence». En KRIMMER 2006a: 39-49.

GONGGRIJP R. y W. J. HENGEVELD
2006 *Nedap/Groenendaal ES3B voting computer: a computer security perspective*, octubre. Disponible en: <http://www.usenix.org/events/evt07/tech/full_papers/gonggrijp/gonggrijp.pdf> (7/12/07; 13:46).

HERNSON, P. et ál.
2006 *The importance of usability testing of voting systems.* University of Maryland. Disponible en: <http://www.usenix.org/events/evt06/tech/full_papers/herrnson/herrnson.pdf> (7/12/07; 20:22).

HITE, R.C. (dir.)
2004 *Electronic voting offers, opportunities and presents challenges,* julio. [Washington D. C.]: US. General Accounting Office.

HOF, S.
2004 «E-voting and biometrics systems?» En: KRIMMER (ed.). *Proceedings: Electronic Voting in Europe,* pp. 63-72. Disponible en: <http://www.e-voting.cc/static/evoting/files/hof_p63-72.pdf> (7/12/07; 18:53).

JEFFERSON D. et ál.
2004 *Analyzing Internet Voting Security,* octubre. Comunicación de la ACM.
2006 *Internet Voting Revisited: Security And Identity Theft Risks of the DoD's Interim Voting Assistance System.* Disponible en: <http://www.ejfi.org/Voting/Voting-35.htm> (7/12/07; 17:20).

Kang, S. y Y. L. Im
2006 «A study on the electronic voting system using blind signature for anonymity». *International Conference on Hybrid Information Technology*, vol. 2 (ichit'06). Washington D. C.: ieee, pp. 660-663.

Keller, A. et ál.
2005 *A PC-based open-source voting machine with an accessible voter-verifiable paper-ballot*. USENIX Association. Disponible en: <http://www.josephhall.org/papers/electronic-voting-machine.pdf> (7/12/07; 20:19).

Kofler, R. et ál.
2004 «The role of digital signature cards en electronic voting». Proceedings of the 37th Hawaii International Conference on System Sciences. ieee. Disponible en: <http://csdl2.computer.org/comp/proceedings/hicss/2004/2056/05/205650116a.pdf> (7/12/07; 19:20).

Kohno, T. et ál.
2003 *Analysis of an Electronic Voting System*. [Baltimore]: Johns Hopkins University.

Krimmer, R.
2006 «Overview». En Krimmer, R. (ed.). *Electronic Voting 2006*. Viena: GI-Edition. Disponible en: <http://www.e-voting.cc/static/evoting/files/krimmer_overview_9-12.pdf> (7/12/07; 13:25).

Krimmer, R. (ed.)
2006a *Electronic Voting 2006. 2nd International Workshop Co-organized by Council of Europe, esf ted, ifip wg 8.5 and E-Voting.*CC. Viena: GI-Edition.

Lambridoudakis, C. et ál.
2003 *Electronic voting systems: security implications of the Administrative Workflow*. ieee. Disponible en: <http://www.instore.gr/evote/evote_end/htm/3public/doc3/public/aegean/paper3.pdf> (7/12/07; 20:14).

MAATEN, E.
2004 «Towards remote e-voting: Estonian case». En KRIMMER 2006a: 81-90. Disponible en: <http://www.e-voting.cc/static/evoting/files/maaten_p81-90.pdf> (7/12/07; 17:02).

MADISE, Ü. y T. MARTENS
2006 *E-voting in Estonia 2005.The first practice of country-wide binding Internet voting in the world.* Tallinn Univ. of Tech. Disponible en: <http://static.twoday.net/evoting/files/madise_martens_estonia2005_13-26.pdf> (7/12/07; 16:59).

MCGALEY M. y J. P. GIBSON
2003 *Electronic Voting: a safety critical system,* marzo. National University of Ireland. Disponible en: <http://www.cs.nuim.ie/~mmcgaley/Download/undergradthesis> (7/12/07; 13:50).
2005 *A critical analysis of the Council of Europe Recommendations on e-voting.* NUI Maynooth (Irlanda). Disponible en: <http://www.usenix.org/events/evt06/tech/full_papers/mcgaley/mcgaley_html/> (7/12/07; 20:25).

MCGALEY M. y J. MCCARTHY
2004 *Transparency and e-Voting Democratic vs. Commercial interests* 2.004 NUI Maynooth (Irlanda). Disponible en: <http://www.cs.nuim.ie/~mmcgaley/Download/Transparency.pdf> (7/12/07; 20:33).

MERCURI, R.
2001 *Rebecca Mercuri's statement on electronic voting.* Disponible en: <http://www.notablesoftware.com/RMstatement.html> (7/12/07; 12:42).

NEWKIRK, GLENN
2004 *US Public Opinion toward Voting Technologies*. Disponible en: <http://www.infosentry.com/US_Public_Opinion_Toward_Voting_Technology_20040301.htm> (13/12/07; 18:29).

PANIZO L. (coord.)
2005 *Así, no* (febrero). Observatorio Voto Electrónico. Disponible en: <http://www.votoelectronico.es/Informes/informes/InformePVI.pdf> (7/12/07; 12:42).

Qadah, G. Z. y R. Taha
2007 «Electronics voting systems: requirements, design and implementation». *Computer Standards & Interfaces,* vol. 29, n.º 3, pp. 376-386.

Ray, I. et ál.
2002 *An anonymous electronic voting protocol for voting over the Internet.* ieee. Disponible en: <http://www.cs.colostate.edu/~iray/research/wecwis01.pdf> (7/12/07; 17:31).

Reingold, H.
1993 *The virtual Community: homesteading on the electronic frontier.* Massachusetts: Addison-Wesley Pub. Co.

Riera A. y G. Cervelló
2004 «Experimentation on secure Internet voting in Spain». En: Krimmer (ed.). *Proceedings: Electronic Voting in Europe,* pp. 91-100. Disponible en: <http://www.e-voting.cc/static/evoting/files/riera_cervello_p91-100.pdf> (7/12/07; 12:42).

Rubin, A.
2006 *Brave new ballot. The battle to safeguard democracy in the age of electronic voting.* Nueva York: Morgan Road Books.

Rüdiger, G. et ál.
2006 «Security requirements for non-political Internet voting». En: Krimmer 2006a: 203-212. Disponible en: <http://www.e-voting.cc/static/evoting/files/grimm_sec_requirements_203-212.pdf> (7/12/07; 20:36).

Sandikkaya, M. y B. Orencik
2007 «Agent-based offline electronic voting». *International Journal of Social Sciences,* vol. 1, n.º 4, pp. 259-263.

Schryen, G.
2003 *E-Democracy: Internet Voting.* Proceedings of the IADIS International Conference.
2004a *Security aspects of Internet Voting.* Proceedings of the 37th Hawaii International Conference on Systems Sciences (hicss'04) - Track 5, p. 50116b.

SCHRYEN, G.
2004b «How security problems can compromise remote Internet voting systems En KRIMMER 2006a: 121-131. Disponible en: <http://www.e-voting.cc/static/evoting/files/schryen_p121-131.pdf> (7/12/07; 18:08).

SKAGESTEIN, G. et ál.
2006 «How to create trust in electronic voting over an untrusted platform». En KRIMMER, R. (ed.). *Electronic Voting 2006*. Viena: GI-Edition.

STOKES, Jon
2006 «How to steal an election by hacking the vote». Disponible en: <http://arstechnica.com/articles/culture/evoting.ars/1> (13/12/07; 18:36).

VOLKAMER M. y R. GRIMM
2006 «Multiple casts in online voting: analyzing chances». En KRIMMER 2006a: 97-106. Disponible en: <http://www.e-voting.cc/static/evoting/files/Volkamer_Grimm_Multiple_Casts_97_106.pdf> (7/12/07; 18:08).

WANG, C. y H. LEUNG
2004 «A secure and fully private Borda voting protocol with Universal verifiability». *Computer Software and Applications Conference, COMPSAC 2004. Proceedings of the 28th Annual International* vol. 28-30, pp. 224-229.

WU C. K. y R. SANKARANARAYANA
2002 *Internet voting: Concerns and solutions*. Cyber Worlds: Proceedings of the first International Symposium on Cyberworlds (CW'02), pp. 261-266.

XENAKIS, A.
2006 «A generic re-engineering methodology for the organized redesign of the electoral process to an e-electoral process». En KRIMMER 2006a: 119-130. Disponible en: <http://www.e-voting.cc/static/evoting/files/Xenakis_Macintosh_BPR_in_E-Voting_119-130.pdf> (7/12/07; 20:06).

Xenakis, A. y A. Macintosh
2004 «Procedural security in electronic voting». *Proceedings of the 37th Hawaii International Conference on System Sciences*. Disponible en: <http://csdl2.computer.org/comp/proceedings/hicss/2004/2056/05/205650116c.pdf> (7/12/07; 20:11).

**Enlaces en Internet**

- Ace. The Electoral Knowledge Network: <http://aceproject.org/ace-en/focus/e-voting/countries>.
- Analysis of an Electronic Voting System: <http://avirubin.com/vote/response.html>.
- Avi Rubin blog: <http://avi-rubin.blogspot.com/>.
- Berry Schoenmakers: <http://www.win.tue.nl/~berry/>.
- Bluescreendemocracy.org: <http://www.bluescreendemocracy.org/archive/1988/aug/saltman.php>.
- Brave New Ballot: <http://www.bravenewballot.org/praise/>.
- California Secretary of State Debra Bowen: <http://www.ss.ca.gov/elections/elections_vst_summit.htm>.
- Commission on Electronic Voting: <http://www.cev.ie/htm/report/view_report.htm>.
- Communities and Local Government: <http://www.communities.gov.uk/corporate/>.
- Consejo Nacional Electoral, República Bolivariana de Venezuela: <http://www.cne.gov.ve/noticiaDetallada.php?id=3608>.
- Council of Europe (e-voting): <http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/>.
- Council of Europe (Recomendación del Comité de Ministros): <http://www.coe.int/t/e/integrated_projects/democracy/02_activities/02_e-voting/01_recommendation/04E-voting%20Rec%20Spanish%20-Traducci%C3%B3n%20Rec%202004%2011%20Comit%C3%A9%20Mins%20Consejo%20Europa.asp>.
- CyberVote (publications): <http://www.eucybervote.org/publications.html>.
- CyberVote (reports): <http://www.eucybervote.org/reports.html>.
- E voting.CC: <http://evoting.twoday.net/>.
- E-Democracia: <http://www.edemocracia.com>.

- Electronic Votin Page (papers): <http://www.social-informatics.net/evoting.htm>.
- Electronic Voting (Rebecca Mercuri): <http://www.notablesoftware.com/evote.html>.
- Electronic Voting Hot List: <http://lorrie.cranor.org/voting/hotlist.html>.
- Electronic Voting Page (news): <http://www.social-informatics.net/evotingnews.html>.
- Electronic Voting Page (papers): <http://www.social-informatics.net/evoting.htm>.
- European WeC Symposium on eGovernment (en español):<http://www.w3c.es/Eventos/2007/eGov/>.
- E-Vote/Clerck: <http://www.deliberate.com/index.html>.
- E-voting security: <http://avirubin.com/vote/>.
- Experience, Reliability, Security & Innovation: <http://www.essvote.com/HTML/home.html>.
- Federal Election Commission (hava 2002): <http://www.fec.gov/hava/hava.htm>.
- First European Conference on Voting, Rating, Annotation: <http://www.deliberate.com/w4g/conf97/fullfreedom.html>.
- Florida, Department of States Division of Elections: <http://enight.dos.state.fl.us/dreinfo/dreinformation.shtml>.
- Ieee (Networking the World): <http://grouper.ieee.org/groups/scc38/1583/index.htm>.
- Informationhere.info (Internet Estonia): <http://www.informationhere.info/internet-estonia.htm>.
- Jason Kitcat (e-voting): <http://www.j-dom.org/h/n/LINKS/evoting/ALL///>.
- Lichfield District Council: <http://www.lichfielddc.gov.uk/site/scripts/search_results.php?searchQuery=default>.
- Lorrie Faith Cranor: <http://lorrie.cranor.org/>.
- Museums, Libraries and Archives Council: <http://www.mla.gov.uk/>.
- National Institute of Standards and Technology (Impoving U.S. Voting Systems): <http://vote.nist.gov/>.
- National Software Reference Library: <http://www.nsrl.nist.gov/vote.html>.
- Nijmeegs Instituut Voor Informatica en Informatiekunde Security of Systems: <http://www.sos.cs.ru.nl/research/society/voting/index.html>.

- Nist and the Help America Vote Act (hava):<http://vote.nist.gov/>.
- Observatorio de Voto Electrónico: <http://www.votoelectronico.es/>.
- OEA-Riter.org: <http://www.oea-rite.org/PagEst_Not_VEOtroPais.htm>.
- Ordinateurs-de-vote-org: <http://www.ordinateurs-de-vote.org/About-us.html>.
- Pippa Norris Articles, John F. Kennedy Scholl of Government, Harvard University: <http://ksghome.harvard.edu/~pnorris/Articles/Articles%20conference%20papers.htm>.
- Própolis. Reflexionamos sobre egovernment: <http://www.propolisclub.net/experiencias.asp?tematica_id=5>.
- Public Law (Help America Vote Act): <http://www.vote.caltech.edu/links/HAVA.pdf>.
- Republique et Canton de Geneve (e-voting): <http://www.geneve.ch/evoting/english/welcome.asp>.
- The Case of the Diebold FTP Site: <http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html>.
- The Electoral Commission (Report on electoral administration published): <http://www.electoralcommission.org.uk/>.
- The Electoral Commission (Modernising Elections): <http://www.electoralcommission.org.uk/elections/modernisingelections.cfm>.
- The Requirements of New York's "Full-Face Ballot" Law: <http://www.wheresthepaper.org/BrennanCtr11_16FullFace.htm>.
- The White House (The National Strategy to Secure Cyberspace): <http://www.whitehouse.gov/pcipb/>.
- Unión Europea (Misión de observación electoral): <http://www.eueomvenezuela.org/contact.html>
- United States. Election Assistance Commission (Glossary): <http://guidelines.kennesaw.edu/vvsg/glossary.asp>.
- United States. Election Assistance Commission (Voluntary Voting System Guidelines): <http://guidelines.kennesaw.edu/vvsg/intro.asp>.
- United States. Election Assistance Commission / Research, Resources and Reports: <http://www.eac.gov/election_resources/vss.html>.
- Usability Professionals' Association: <http://www.upassoc.org/upa_projects/voting_and_usability/uk-evoting.html>.
- Venelogía: <http://www.venezolano.web.ve/archives/733-Informe-de-la-OEA-sobre-elecciones-parlamentarias-en-Venezuela.html>.

- Verified Voting Foundation: <http://www.verifiedvotingfoundation.org/article.php?id=6289>.
- VLex (Voto Electrónico): <http://premium.vlex.com/actualidad/especiales/Voto_Electronico/2500-VEL,05.html>.
- Voto Electrónico (Resultados): <http://www.votoelectronico.pt/index.php?option=com_content&task=category&sectionid=6&id=79&Itemid=84>.
- Voto-e (Artigos e Textos sobre Voto Eletrônico) <http://www.brunazo.eng.br/voto-e/textos/index.htm>.
- Voto Telemático: <http://vototelematico.diatel.ump.es>.
- Wijvertrouwenstem computersniet: <http://www.wijvertrouwenstemcomputersniet.nl/English>.
- Wikipedia (The Free Encyclopedia): <http://en.wikipedia.org/wiki/2004_United_States_presidential_election_controversy%2C_voting_machines#Specific_issues_relating_to_Diebold_machines_and_practices>.
- Wired: <http://www.wired.com/politics/security/news/2007/03/72846>.

# Sobre el autor

Luis Panizo nació en León (España) y se graduó en Ingeniería de Telecomunicación por la Universidad Politécnica de Madrid (1975-1980). Realizó cursos de posgrado en la misma Universidad relacionados con la programación en lenguaje ensamblador y sistemas operativos.

Entre 1980 y 1984 ocupó en su país varios puestos de alta responsabilidad técnica en diversos Ministerios (Interior, Hacienda, Sanidad e Industria).

En 1985 accedió a una plaza de profesor ayudante en la Universidad de León y en 1987 se adscribe a la plaza de profesor titular en el área de Arquitectura y Tecnología de Computadores, cátedra que ocupa hasta hoy. Ha impartido docencia en diversas universidades españolas y extranjeras sobre distintas materias relacionadas con los sistemas operativos, la arquitectura de computadores y la seguridad informática. Fue director del Departamento de Ingeniería Eléctrica y Electrónica de la Universidad de León durante ocho años.

Ha dirigido varios contratos de investigación con organismos y empresas, entre los que destaca el suscrito con el Procurador del Común (Defensor del Pueblo) en Castilla y León. Actualmente coordina el grupo de investigación sobre accesibilidad del Instituto Nacional de Tecnologías de la Comunicación (INTECO).

Ha recibido el premio Chip de Oro otorgado por Radio Nacional de España por su labor divulgativa en las tecnologías de la información y las comunicaciones.

Tiene diversas publicaciones personales en revistas de impacto global y ha sido editor principal de varios simposios internacionales sobre informática.

Lleva cinco años estudiando las tecnologías sobre voto electrónico presencial y remoto; se desempeña como observador en diversos procesos electorales nacionales e internacionales, emitiendo los correspondientes informes.

Es secretario del Observatorio de Voto Electrónico de España.