**Libro blanco del voto electrónico**

Luis Panizo Alonso

Observatorio del Voto Electrónico

Diciembre, 2013

# Índice

Índice de figuras 3

Códigos de acrónimos 3

1. Presentación 5

2. Objetivos 6

3. ¿Qué es el voto electrónico? 6

4. Clasificación y tipología del voto electrónico 6

5. Las oportunidades del voto electrónico 10

6. Aspectos esenciales 12

6.1 Consideraciones generales 12

6.2 El problema de la seguridad 14

7. Uso mundial del voto electrónico 19

7.1 Visión general 19

7.2 Experiencias más relevantes y sus debilidades: Venezuela, Brasil y la India 24

7.3 Iniciativas europeas 30

7.4 Iniciativas y experiencias españolas 31

7.5 Experiencias de voto telemático o remoto 32

7.6 Conclusiones de las experiencias mundiales 34

8. Empresas y productos 34

9. Estándares 38

10. Propuestas y recomendaciones 39

11. Referencias y documentación 42

# Índice de figuras

Figura 1 Voto de una urna con OCR (USA) 9

Figura 2 DRE con VVPAT 11

Figura 3 DRE con lector de tarjeta 15

Figura 4 Cifrado gráfico del voto (Chaum) 18

Figura 5 Justificación del recibo de voto 18

Figura 6 Voto en papel perforado (USA) 21

Figura 7 Urna de Coahuila (Méjico) 23

Figura 8 Urna de Jalisco (Méjico) 23

Figura 9 Segundo paso: voto clásico 24

Figura 10 Tipos de DRE en Venezuela 25

Figura 11 DRE de Brasil con lector de huellas 26

Figura 12 DRE Brasileña 27

Figura 13 Aspecto de la votación en la India 28

Figura 14 DRE de la India 28

Figura 15 El Dr. Halderman y sus colaboradores 29

Figura 16 Programa Pnyx de Scytl 34

Figura 17 DRE de Indra 36

Figura 18 Dos tipos de DRE de Diebold, con VVPAT (sin acceso) y con lector de identidad 37

# Códigos de acrónimos

ANSI Instituto Nacional Estadounidense de Estándares

CoE Consejo Europeo

CSFE Consejo Superior de Franceses en el Extranjero

DNI Documento Nacional de Identidad

DRE *Direct-recording* electronic voting *machine.* Urna electrónica.

E2E End-to-end auditable voting system. Auditoría completa e indirecta del sistema de votación por procedimientos de cifrado*.***End-to-end auditable voting systems**

EAC Comisión de asistencia para las elecciones americanas.

EPC Elecciones al Parlamento de Cataluña

EU Unión Europea

EVM *Electronic Voting Machines.* Equipos de votación electrónica.

EVS *Electronic Voting Systems.* Sistemas de votación electrónica.

e-vote *Electronic-vote.* Voto electronico.

FAQ Preguntas frecuentes

FEC *Federal Election Commission.* Comisión federal electoral de EE.UU.

FTP Protocolo para transferencia de archivos.

GNU-GPL Licencia general de una aplicación para hacerla de distribución pública.

GST Grupo de Seguimiento Técnico de Venezuela.

HAVA Help America Vote Act. Ley federal para promover estándares mínimos en las elecciones en EE.UU.

IEEE Institute of Electrical and Electronics Engineers. Asociación Americana de Ingenieros Eléctricos y Electrónicos.

ISO Organismo Internacional de normalización.

ITA Information Technology Association. Asociación de empresas de Tecnologías de la Información.

i-vote Internet-vote. Voto por Internet o telemático.

NASED National Association of State Election Directors. Asociación Nacional Americana de responsables electorales de los Estados.

NIST National Institute of Standards and Technology. Instituto Americano de normalización y tecnología.

OCR Reconocimiento óptico de caracteres.

OVE Observatorio del voto electrónico (España).

PC Ordenador personal.

PDA Agenda electrónica de bolsillo.

PKI Infraestructura de clave pública.

Rec Recomendación Europea.

RIES Rijnland Internet Election System. Sistema de votación telemática con auditoría tipo E2E.

SERVE Secure Electronic Registration and Voting Experiment (2004).

TCP/IP Protocolo de comunicación de Internet.

TIC Tecnologías de la Información y las Comunicaciones.

VE Voto electrónico.

VSS Voting system standards. Normalización de los sistemas de votación.

VVAT Voter Verified Audit Trail. Sistema de auditoría mediante verificación por parte del votante.

VVPAT Voter Verified Paper Audit Trail. . Sistema de auditoría mediante emisión del voto en papel para verificación por parte del votante.

"Things should be made as simple as possible, but no simpler."

Atribuida a Albert Einstein

“Lo que veo aquí es sólo una corteza. Lo más importante es invisible…”.

Antoine de Saint-Exupéry en El Principito

# 1. Presentación

Han sido muchas las iniciativas que se han realizado en diversos países para avanzar en lo que ha venido en llamarse e-democracia o democracia electrónica y especialmente en el campo del voto electrónico. Ambos términos, democracia electrónica y voto electrónico, se utilizan con profusión y no siempre con el mismo significado para todos y por ello es conveniente delimitarlo y precisarlo. Por democracia electrónica se entiende el uso de las tecnologías de la información y las comunicaciones (TIC) para favorecer y mejorar la participación ciudadana en los procesos de consulta y decisión que caracterizan a los sistemas políticos democráticos. El concepto por tanto incluye todos los procesos electorales y votaciones habituales utilizados para elegir a los representantes políticos en los distintos niveles administrativos -que en nuestro país son tres, estatales, autonómicos y locales- pero también cualquier otro proceso de participación ciudadana en la toma de decisiones de las administraciones y que puede formularse a través de procesos de consulta a los ciudadanos, tipo referéndum, o mediante recogidas de opinión por medios electrónicos sobre algún tema de interés. En cambio el término voto electrónico se centra en el uso de estas tecnologías en el desarrollo de una votación, tenga ésta el nivel de relevancia que tenga. Es evidente que el voto electrónico es la herramienta fundamental para posibilitar la democracia electrónica pero no es la única. A su vez el voto electrónico puede utilizarse en otros ámbitos que no son los procesos electorales de las administraciones públicas, así puede ser útil en los procesos electorales de cualquier organización, empresa o sociedad privada y es aquí donde puede tener mayor utilidad por requerir menos condiciones operativas.

Las TIC pueden ser útiles en cualquiera de las fases que constituyen el proceso habitual de unas elecciones; pueden serlo en la elaboración del censo, en la identificación del votante, en el proceso de depositar el voto o en el escrutinio final. En algunas de esas etapas ya se usan habitualmente estas tecnologías y así se ve como normal que el censo electoral se almacene y se procese por medio de bases de datos electrónicas y aunque es probable que éste proceso podría ser mejorado aprovechando más las facilidades que ofrecen los computadores y las redes de comunicación, las administraciones asumen que el uso de bases de datos es el mejor mecanismo de gestión de estos. Muy diferente es la situación en las otras fases del proceso electoral. El proceso de identificación del votante y la consiguiente limitación de un voto por votante, se realiza en nuestro país por medio del documento nacional de identidad (DNI). La Administración Central está realizando en la actualidad un proceso para la implantación del DNI electrónico pero no se han explotado todas las posibilidades de su uso para la identificación electrónica ya que la solución propuesta le asegura la compatibilidad con el DNI antiguo y por tanto está siendo utilizado de forma mayoritaria de la forma más clásica. En cuanto al proceso de depositar el voto, el método sigue siendo en la mayor parte de los casos la urna tradicional y para el recuento de los votos la utilización de los ordenadores se limita a un papel de centralización de datos y elaboración de informes oficiales de resultados.

Este documento pretende dar a conocer el porqué es tan difícil hacer las cosas bien en el entorno del voto electrónico, cuáles son las razones y cómo podemos conseguir un uso correcto y sencillo de las tecnologías actuales en los diversos ámbitos de aplicación del voto electrónico en nuestra sociedad. Para ello se van a analizar y a clasificar las diversas soluciones propuestas por empresas y desarrolladores con el objeto de conocer el grado de cumplimiento con los requisitos necesarios en los procesos con base democrática.

Se pretende simplificar para lograr confianza en el voto electrónico. Hasta el momento esto no se ha conseguido debido a los intereses encontrados entre los cuatro actores que han intervenido en el panorama del voto electrónico. Desde nuestro punto de vista han sido: las empresas desarrolladoras de sistemas y soluciones, los Estados que han creado sus propios equipos y desarrollos, la comunidad científica que llevan décadas haciendo propuestas y mejoras y, por último, los ciudadanos que han intervenido en su uso y valoración.

# 2. Objetivos

Analizaremos los casos más significativos, cómo han sido propuestos, cómo se han desarrollado y, si fuera el caso, cómo se han auditado. Nos interesa conocer los inconvenientes, las críticas, los análisis de los investigadores, las propuestas de mejora, todo con el afán de diseñar y utilizar sistemas de votación electrónica que cumplan con todos los requisitos esenciales para que sean vistos con la misma transparencia y seguridad que los comicios celebrados con una urna convencional.

Nos preocupa dejar claro cuáles son los aspectos a verificar antes de proponer un sistema y el procedimiento posterior que nos permita comprobar su transparencia y cumplimiento con los aspectos básicos de cualquier proceso democrático. No nos debe cegar el impulso de imponer la tecnología en el ámbito democrático a cualquier precio o por considerar que es uno más de los entornos que pueden digitalizarse.

Además, se relacionan las soluciones más comunes a los problemas creados y qué problemas todavía no han sido superados de forma clara debido a los complejos retos que son consustanciales a ellos.

# 3. ¿Qué es el voto electrónico?

El Consejo de Europa [1] define “voto electrónico” (VE) como aquel donde al menos el voto es emitido por medios electrónicos. Esta definición no es muy clara si queremos realizar un estudio en profundidad y necesita ser matizada, tanto en sus aspectos tecnológicos como sociales [2].

# 4. Clasificación y tipología del voto electrónico

En un tema de actualidad tecnológica como el que nos ocupa es frecuente la utilización de término ingleses y su traducción al español no siempre es directa. Comenzamos pues definiendo la terminología básica que vamos a utilizar en este documento ya que existen tres conceptos que son confundidos con frecuencia: los que tienen que ver con las elecciones electrónicas, las urnas electrónicas y el voto electrónico.

Urna electrónica: equipo electrónico que permite recoger un voto por algún medio electrónico y que ha sido diseñado y construido con ese fin. Existen sistemas de urna electrónica que han probado su eficiencia y correcto funcionamiento en la práctica. Muchas veces se utilizan los términos de voto electrónico y de elección electrónica como recurso publicitario, cuando realmente se refieren apenas a una urna electrónica. Puede estar conectada a la red (*on-line*) o no (*off-line*). También se conocen en el mundo anglosajón con las siglas DRE (*direct-recording electronic*), algo así como “grabación electrónica directa”, al referirse a la grabación sobre un soporte digital de información.

Voto electrónico (*e-vote*): voto emitido desde un medio digital -que puede ser a través de un ordenador de sobremesa o de una urna electrónica-, que puede ser transmitido a través de un medio telemático y recogido y contabilizado utilizando un medio informático.

Sistema de votación electrónica (*electronic voting system*) (EVS): sistema de votación que involucra, al menos, el proceso de elección, el depósito del voto y el proceso de contabilidad de los mismos, utilizando para ello medios electrónicos basados en computadores y redes de comunicación.

Votación telemática (*remote electronic voting o i-vote*): proceso de votación que puede realizarse desde cualquier lugar físico en el que se disponga del dispositivo electrónico adecuado, bien sea un ordenador, una *tablet,*  un teléfono móvil, agendas electrónicas, etc. Algunos autores lo denominan voto remoto pero este puede ser el voto por correo, por lo que sería necesario añadir el término electrónico y por tanto utilizar una descripción como votación electrónica remota que sería **equivalente**.

Votación electrónica presencial en colegio electoral (*poll site electronic voting*): proceso de votación que conlleva el uso de medios electrónicos para la selección, registro, almacenamiento y recuento de los votos pero que se realiza en un lugar público como un colegio electoral vigilado y controlado.

Votación en quiosco (*kiosk voting*): votación realizada en un colegio electoral, es decir en un lugar público vigilado y controlado, pero el voto se transmite por una red, o dicho de otro modo el kiosco está conectado a una red.

Sistema de votación utilizando grabación electrónica directa del voto (DRE): sistemas que se basan en diferentes formas de urnas electrónicas, en las cuales el elector hace su selección directamente sobre un dispositivo electrónico y el voto es almacenado digitalmente.

Escrutinio electrónico (*electronic counting*): proceso de recuento en el que se ven implicadas tecnologías electrónicas, ya sea para contar votos digitales (ceros y unos), como para votos en otros soportes (papeletas para lectura óptica) (OCR).

Prueba para verificar el voto emitido (*voter-verified audit trail o VVAT*): prueba que emite una urna electrónica con el objeto de verificar el voto emitido.

Recibo en papel para verificar el voto emitido (*voter-verified paper audit trail o VVPAT*): recibo de papel que emite una urna electrónica con el objeto de verificar el voto emitido.

Votación en línea (*online voting*): la que se realiza sobre cualquier conexión electrónica contra un sistema en funcionamiento, de forma que el voto es procesado en ese mismo instante, aunque los resultados se hagan públicos posteriormente.

Voto por Internet (*Internet voting* *o i-voting*): es un caso específico de voto telemático cuando este se desarrolla exclusivamente sobre la red de redes.

Servidor de votación (*server voting*): término genérico para identificar el ordenador que posibilita la realización de una votación en línea.

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

Así cuando votamos con ayuda de una máquina dispuesta en un lugar específico (colegio electoral) y que para acceder a ella el votante ha de ser identificado previamente de forma manual, y autorizado para utilizar la máquina, que en este caso genéricamente se denomina DRE. Este proceso de votación es presencial y el proceso de identificación es independiente y no debe de existir la posibilidad de relacionarlo con el voto depositado disponiendo de toda la información necesaria “in situ”. Para ello se utilizan equipos específicos.

Por el contrario cuando el voto no es ejercido presencialmente y se lleva a cabo de forma remota utilizando medios telemáticos (votación telemática) y más concretamente Internet, el sistema lo hace todo, es decir, identificar y enviar el voto, con independencia del dispositivo ya sea un ordenador personal o equipamiento equivalente. Por tanto, en este caso el equipo no es específico.

Clasificaciones más amplias permiten ver con más detalle los sistemas utilizados y su evolución:

* Sistemas tradicionales: papeletas, tarjetas perforadas, máquinas de palancas o levas.
* Sistemas de voto electrónico convencionales, genéricamente urnas electrónicas, que pueden ser: urnas con lectores ópticos de caracteres (OCR), los mencionados DRE que en general dispondrán de pantalla táctil y registro de datos en dispositivos basados en semiconductores, magnéticos, ópticos o soluciones híbridas.
* Voto remoto o telemático: que puede ser en quiosco electoral ubicado en cualquier parte, o bien en colegio electoral y sobre cualquier dispositivo con conexión a Internet e incluso desde cualquier parte (voto remoto puro).

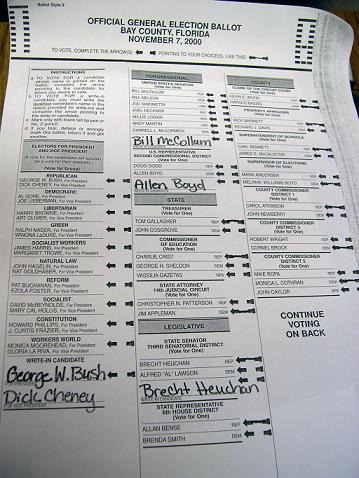


Figura 1 Voto de una urna con OCR (USA)

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 U.S.A. en el 2004 fueron las ópticas seguidas de las DRE. Hoy en día estas últimas son más utilizadas que las primeras.

En cambio el voto remoto puro se ha utilizado en muy pocos países y menos de forma vinculante como ha sido el caso de Estonia en marzo de 2007 y 2011.

Si nos centramos en los dispositivos electrónicos que podemos utilizar en el voto electrónico podemos finalmente clasificarlos en función de su uso controlado y no controlado. En el primer caso podemos tener:

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

Y en el segundo:

* Dispositivos para voto electrónico remoto o telemático (PCs, móviles, PDAs)

Incluso podemos considerar el caso de dispositivos que puedan utilizarse en ambos ambientes, controlados y no controlados:

* Quioscos para voto electrónico conectados a red.

En función de los aspectos automatizados resulta útil establecer una clasificación de los sistemas de votación en tres niveles [3] , tal como se indica a continuación:

En un primer nivel de automatización del proceso electoral que denominaremos básico se utilizan dispositivos electrónicos, herramientas informáticas y medios telemáticos para agilizar los procesos administrativos que tienen que ver con la emisión del voto, como son: el registro de votantes, la generación y publicación del censo electoral, el recuento de papeletas, la impresión de todas las actas necesarias y la transmisión de resultados de votación (independientemente que se utilicen o no otros medios no electrónicos) Este primer nivel puede ser adecuado para aquellos países en los que han funcionado adecuadamente durante tiempo y no se han observado dificultades específicas. Concretamente es el caso de España en el entorno de las elecciones políticas en todos sus niveles, donde se viene a denominar “mesas administradas electrónicamente” [4] .

En el siguiente nivel denominado intermedio se introduce la automatización de los procesos de emisión y recuento del voto. Las urnas convencionales en las que se introducen los votos en papel se sustituyen por sistemas informáticos, denominados equipos o sistemas de grabación electrónica directa, en terminología anglosajona DRE, que capturan y almacenan el voto de forma electrónica y permiten realizar automáticamente el recuento al terminar la votación. Como vamos a poder comprender a lo largo de este documento, estos equipos tienen defensores y detractores y cada uno pone de relieve sus ventajas e inconvenientes. Los ejemplos más importantes de uso están en la India, Brasil y Venezuela [5] [6] [7], donde se han implantado sistemas de voto electrónico con ciertas experiencias en su haber.

Cuando al anterior nivel se le añade el uso de redes telemáticas obtenemos el nivel avanzado de automatización en los procesos electorales. En este caso los votos se depositan en una urna remota sin control del votante. A este caso lo denominamos voto telemático también conocido como voto electrónico (*e-voting*) con cierta frecuencia y puede crear confusión con el anterior [8]. En este nivel está incluido el proceso electoral completo, desde la identificación de cada votante hasta la publicación de los resultados, todo procurando las máximas garantías de seguridad.

# 5. Las oportunidades del voto electrónico

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 estos aspectos son indiscutibles pero otros se dan por seguros incluso sin estudios básicos sobre el tema. En la parte positiva destacan la precisión y la rapidez y en la negativa la falta de seguridad.

Entre los aspectos positivos caben destacar: precisión en la contabilidad de los votos, rapidez en el recuento, incremento de la accesibilidad para discapacitados o por personas con diversidades funcionales, ahorro de papel, flexibilidad, posibilidad de crear una infraestructura permanente para la opinión con voto, mejora de la eficiencia, etc. También se dan por ventajas aspectos más discutibles como pueden ser el ahorro ecológico y la sostenibilidad, ya que las urnas tienen un determinado consumo energético en su fabricación y uso.

Otro aspecto es que su utilización parece ser más barata que el uso de la urna tradicional pero hay pocos estudios serios. Por poner un ejemplo, en una de las últimas elecciones presidenciales con urnas electrónicas celebradas en Venezuela en Diciembre de 2006 el coste estimado por nuestra observación directa fue de 200 millones de dólares. Por otro lado, hay comparativas de costes en U.S.A. [9] [10] [11] con urnas basadas en sistemas con lectura óptica de caracteres (OCR) y urnas electrónicas tipo DRE, 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 coste de la máquina y el del software de forma separada, o bien por voto emitido.

A considerar también está el supuesto aumento de la participación, el cuál este documento no va a analizar [12] [13], como tampoco los problemas jurídicos pendientes de solucionar en la mayor parte de los países, incluido España.

En cuanto a los inconvenientes también son variados y algunos no demostrados como ocurre con lo expresado anteriormente. 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 la opinión pública, de los políticos e incluso de algunos desarrolladores e investigadores, considerar que el nivel de seguridad de una votación electrónica es similar al requerido en una entidad financiera [14], ya que en esta 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, por lo que NADIE puede tener información sobre el voto salvo en el proceso final de recuento y exclusivamente para la contabilidad [15]. Este tipo de inconvenientes nos obligan a utilizar diversas técnicas de verificación del voto como el VVAT o el VVPAT [16] [17]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 [18] [19].



Figura 2 DRE con VVPAT (Smartmatic)

Otro aspecto negativo es el posible fraude que se puede realizar con este tipo de dispositivos. En este caso si hay estudios rigurosos como los de Di Franco [20] que 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 estos aspectos, 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 [21] [22] [23] [24] denuncian el elevado riesgo por el mero uso de Internet (malware, vulnerabilidades, denegación de servicio distribuida, falta de control por las autoridades electorales de los equipos utilizados por los votantes, etc.) y por la baja transparencia del procedimiento incluyendo la posible pérdida del anonimato. Incluso el propio Vinton Cerf, uno de los padres de Internet por su aportación al protocolo TCP/IP, considera que una de las debilidades de la Red es su baja seguridad. 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 de los costes y a la desaparición de votos nulos. El uso de la redes para el voto, a lo que el profesor Carracedo denomina “votación telemática” [8], tiene enormes ventajas por su flexibilidad en el uso pero tiene grandes retos que superar como los riesgos en la seguridad y disponibilidad.

Las tecnologías de voto remoto vía web, tan atractivas e interesantes y que tanta inmediatez proporcionan, nos acercan a lo que la experta y analista Pippa Norris, de la John F. Kennedy School of Government de Harvard University, llama “política total”. La política total, al intervenir acortando prodigiosamente el espacio y el tiempo —proporcionando un grado de sofisticación en la participación imposible de imaginar hace unos pocos años—, actúa sobre los incentivos estratégicos para los partidos, los políticos y los ciudadanos. Impacto que podría cambiar las reglas electorales, que a su vez generarían cambios en los comportamientos políticos para terminar afectando a la intensidad y complejidad de los derechos políticos tal como hoy los conocemos. Internet tiene un intenso impacto sobre los estándares de acción y participación política, razón por sí misma de suficiente entidad como para considerar, con seriedad, la conveniencia de estimular los sistemas de participación y voto telemático, eso sí, prestando especial atención a las garantías y cautelas legales asociadas y a las limitaciones de seguridad propias de este medio.

# 6. Aspectos esenciales

## 6.1 Consideraciones generales

Los medios electrónicos podrían ofrecer muchas ventajas en las diversas fases de la realización de un proceso electoral. Una mayor automatización en la elaboración del censo posibilitaría probablemente un menor número de errores en el mismo, una consulta remota por parte de los ciudadanos y con ello una mayor agilidad en el proceso de rectificación de errores o una mayor sincronización entre las distintas administraciones. La utilización de sistemas electrónicos en el proceso de identificación podría hacer el proceso más fiable y más rápido.

El proceso de depositar el voto podría abaratarse, agilizarse o hacerse más cercano a personas discapacitadas o con problemas con el idioma utilizado en el sistema de votación. También podría mejorarse el proceso de voto remoto basado actualmente en voto por correo ordinario. Por último, el proceso de escrutinio de votos podría agilizarse enormemente utilizando las Tecnologías de la Información y Comunicaciones (TIC).

Las posibles ventajas enumeradas en los párrafos anteriores son eso, posibles, y no deberían conducirnos al error de pensar que se alcanzarán sea cual sea la solución de voto electrónico que se adopte. Por el contrario son varios los ejemplos en los que la implantación de un sistema de voto electrónico ha conllevado más problemas que ventajas. Y es que, además del reto que supone encontrar soluciones que concreten las hipotéticas ventajas de los nuevos sistemas de voto electrónico en ventajas reales, son a su vez muchos los nuevos problemas que pueden surgir al adoptarlos. Por ejemplo, se plantean problemas de seguridad a la hora de proteger los datos, tanto del censo como de los votos; se plantean problemas de transparencia ya que las nuevas tecnologías podrían hacer opaco el sistema de votación y generar desconfianzas sobre el valor del voto realizado o el mantenimiento de la anonimia del mismo; se plantean problemas de auditoría y verificación a nivel individual y general de los procesos electorales; se plantean problemas de integridad de los datos, teniendo la necesidad de asegurar que sólo las personas autorizadas tienen acceso a los datos de la votación y que estos no pueden ser modificados; se plantean en fin un conjunto de nuevos problemas que el sistema tradicional ya tiene asumidos o resueltos pero que surgen al cambiar el sistema de votación. Por eso cualquier solución informática de voto electrónico tiene que ser sometida a un cuidado diseño, que incluyan un buen conjunto de pruebas y con una puesta en funcionamiento correcta y paulatina.

Por todo ello es necesario garantizar una serie de aspectos en el voto electrónico para conseguir que cumpla con los requisitos que imponen los sistemas democráticos lo que hace que las posibles soluciones sean cuando menos complejas. Estos requisitos han sido descritos por diversos autores y desde puntos de vista muy variados [17] [25] [26] [27] [28] [29] [30].

Estos son:

1. Autenticación: que sólo los que estén legitimados para votar, voten.
2. Unicidad del voto: que sólo se pueda votar una vez.
3. Anonimato: que no se pueda relacionar el votante con el voto.
4. Imposibilidad de coacción: el votante no puede en ningún caso ser capaz de demostrar qué voto emitió, impidiendo la compra masiva de votos y la presión (coacción) sobre los votantes.
5. Precisión: el sistema tiene que poder 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 está 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 periodo de votación. De esta forma se evita que los resultados parciales afecten a la decisión de los votantes que no han votado.
8. Auditabilidad: que existan procedimientos para poder verificar que todos y cada uno de los componentes físicos y lógicos utilizados para votar funcionan correctamente.
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 de ser flexibles con los formatos utilizados (idiomas, posibles elecciones a distintos órganos, diversos tipos de papeletas de votación) y ser compatibles con todo tipo de plataformas y tecnologías.
11. Accesibilidad: que permita ejercer el voto a personas con diversidad 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 coste: 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, impidiendo la manipulación de los votos a todos los niveles.
16. Compatible con la tradición electoral y por tanto que se parezca lo más posible a una urna convencional en su aspecto y utilización.
17. Abierto, de forma que las autoridades electorales y si es el caso el ciudadano, puedan obtener detalles de su funcionamiento (hardware y software).
18. Barato, de forma que sea competitivo con el voto tradicional.

Sin duda que el cumplimiento en mayor o menor grado está en función de los diversos puntos de vista de los elementos involucrados: administración, ciudadanos (electores), empresas y la de Academia. De esta forma la administración en general opina que los procesos electorales son complejos, costosos y en algunos casos poco eficientes y problemáticos, por lo que intentan utilizar las TIC para su simplificación, mejora y abaratamiento. Los ciudadanos observan que los métodos utilizados son arcaicos y en algún caso poco fiables (papeletas perforadas en el estado de Florida en Noviembre del 2000, voto por correo en la mayor parte de los países, etc.) pero no están seguros que los nuevos métodos usando las tecnologías informáticas cumplan los requisitos imprescindibles. Las empresas que ven una oportunidad de negocio ofreciendo máquinas que cumplen con su cometido y muy probablemente bien desarrolladas, pero con escaso control por parte del contratante e intentando mantener la solución como una “caja negra” y con pocas posibilidades de verificación desde el exterior. La Academia que ve todo esto como un reto científico y tecnológico e intenta desarrollar soluciones que minimicen los problemas y garanticen el cumplimiento de los requisitos necesarios.

## 6.2 El problema de la seguridad

Habitualmente se ignora que los requerimientos de seguridad más altos que se conocen son de necesaria aplicación en las infraestructuras de voto electrónico, por las exigencias legales y democráticas que deben satisfacer. El valor del voto es secreto de manera absoluta y nadie, absolutamente nadie, está autorizado a unir el valor del voto y la identidad del votante. El voto es el dato con mayor grado de protección jurídica de todos los existentes. Ninguna otra tecnología está pensada para satisfacer un requisito tan alto. El secreto es absoluto y no existe vía legal de escape o privilegios específicos a personas o autoridades para unir valor del voto e identidad del votante. No existen. Los secretos de estado, las armas de destrucción masiva, víricas, bacteriológicas, químicas o bases de datos sensibles que hace posible la fabricación de armas de destrucción masiva, están sometidas a privilegios de acceso para personas y autoridades. No es el caso de las infraestructuras de voto electrónico. Tienen que garantizar el secreto de manera absoluta. El valor del voto es un atributo indivisible de su autor.



Figura DRE con lector de tarjeta

No decimos que las dificultades de seguridad sean menores para organizar el acceso selectivo a las armas de destrucción masiva o las bases de datos muy sensibles. Los procedimientos de seguridad y las exigencias tecnológicas y de procedimiento de dichos sistemas, son demandantes de primer nivel de recursos tecnológicos y científicos. Lo que se dice es que las infraestructuras de voto electrónico están asociadas a los requerimientos de seguridad en los protocolos y en la ingeniería de software y hardware más altas que se conocen, en justa proporción a su elevada utilidad social y a la correspondiente sensibilidad social ante dichas tecnologías. Está en juego, nada más y nada menos, la credibilidad de las instituciones que hacen posible la nación política y de las que, en grado muy alto en las sociedades avanzadas, depende la prosperidad de las respectivas sociedades.

Históricamente se cometió el error de considerar que la seguridad necesaria en un proceso electoral no era más complejo que el necesario para controlar la aviónica de un aeroplano o la seguridad bancaria. Son analogías incorrectas. [15]

Es por ello que el problema de seguridad que conlleva el voto electrónico es único. Históricamente esta realidad ha sido relegada o sencillamente no considerada en las diversas soluciones tecnológicas aportadas por los implicados en la puesta en marcha de este tipo de infraestructuras.

Todos estos riesgos de seguridad han sido analizados y divulgados en diversos estudios por los más destacados expertos [31] [21] [32]. En este sentido hemos avanzado mucho en la búsqueda de una solución que satisfaga todos los requisitos necesarios y a todos los responsables de estos procesos. Si bien es cierto que inicialmente se ha confiado en el buen hacer de los expertos, ya fueran empresas o Estados, el tiempo nos ha obligado a establecer procedimientos de auditoría. Estas auditorías han resultado complejas, largas, pocos claras y sin estándares claramente definidos, que incluso nos han llevado a discusiones inacabables como ha sido determinar si deberían ser abiertas o no. El secreto del voto, tanto de lo que se vota como de quién lo realiza, está en conflicto con los procesos de auditoría necesarios para generar confianza y es aquí donde aparece como necesarias las técnicas de cifrado y codificado, también conocidas como criptografía en término anglosajón.

Ha sido habitual que los procesos electorales apoyados en tecnología, en mayor o menor grado, carecieran de transparencia en parte del proceso. Generalmente el fabricante de la solución electrónica para la votación imponía una “caja negra” entre el depósito del voto y el recuento. Han sido numerosos y diversos los ejemplos de un uso incorrecto de este tipo de soluciones [33] [34] que han contribuido a generar dudas y no pocos detractores [31] [35]. En una palabra, en vez de generar confianza han incrementado las dudas.

¿Por qué es tan complejo el voto electrónico seguro y verificable?

Son varios los aspectos que confieren al voto electrónico una dificultad única para poder ser resuelto con plenas garantías democráticas [36]. Estos pueden clasificarse en: intereses creados, tipo de adversarios y dificultad para detectar y recuperar fallos.

El interés en manipular unos resultados electorales son evidentes ya sea por las ventajas sociales, económicas o políticas que podríamos obtener [37].

Los adversarios que pueden atacar un proceso electoral son muy amplios, desde el propio votante, las autoridades, los organizadores o cualquier tipo de unión entre ellos. Es decir, no están delimitados ni aislados como puede ocurrir en otros casos como en la banca o en la aviación donde estos riesgos están más acotados, estudiados y aislados, con opciones de auditoría y verificación por parte de un tercero. Además en el caso de las votaciones nadie puede observar los ataques desde dentro del sistema cuando este está en marcha, lo que complica enormemente la detección de manipulaciones y errores.

En la votación electrónica es imposible recuperar un error una vez que el voto ha sido emitido o bien cuando se verifica que el recuento ha sido incorrecto. La única posibilidad es repetir el proceso de votación. En aviación existen las cajas negras que nos indican mediante registro de todos los datos donde se han producidos los errores con objeto de corregirlos y que no vuelva a ocurrir. Al igual que en la banca mediante recibos de las operaciones. En el voto electrónico no es posible este tipo de control por lo que la detección de los errores se efectúa tarde o nunca y la posibilidad de aislar el problema no existe ya que lo desconocemos. Además si lo detectamos lo único que podemos hacer es repetir el proceso de votación desde el comienzo o conformarnos con el resultado aunque no respete la esencia democrática [32].

En primer lugar apareció como propuesta el VVPAT [17] o prueba de auditoria en papel para verificación del votante, lo que complica y ralentiza el uso de las máquinas y el recuento posterior de los votos, además de descubrir nuevas vulnerabilidades [15]. A pesar de todo hay claras limitaciones en la seguridad de estos equipos ya que pueden dar paso a la posibilidad de la coacción sobre el votante en el sentido de que exista una prueba física del voto que imposibilita la marcha atrás en el sentido del voto y que puede ser demostrada con una simple fotografía tomada por el votante, o bien si se dispusiera de una papeleta oficial se podría poner en marcha una cadena de coacciones.

Posteriormente se propusieron las auditorías que implicaban la revisión de todos los elementos implicados en el proceso [25] [38], y el propio proceso en si desde su diseño, el despliegue, la realización y el cierre. Para ello fue necesario determinar todos los aspectos a auditar y el cómo debería realizarse, por lo que se vieron obligados a crear unas normas y un procedimiento, lo que no resultó sencillo. Después apareció el debate de quién lo debería llevar a cabo y de qué forma trasladar los resultados a los ciudadanos y por tanto si debería ser abierto o no [39].

Que todo esto no nos desanime pues hay suficiente conocimiento para diseñar procesos de votación electrónica razonablemente seguros y fiables. Está claro que todo se basa en generar CONFIANZA en el electorado y esto no se consigue de un día para otro.

Si bien es cierto que las técnicas de cifrado pueden ser una excelente aliada para resolver problemas que parecen imposibles, no es menos cierto que la verificación de un proceso electoral es más complejo de lo que parece. En este sentido vamos a intentar demostrar que votar es un problema único de generar confianza, que estas técnicas bien aplicadas nos pueden ayudar a conseguirla y que el único camino correcto es utilizar métodos de verificación abierta tanto a nivel individual como general. Hoy por hoy la única salida posible para cumplir con los requisitos esenciales del voto democrático es el uso de diversas técnicas de verificación del voto que vamos a exponer a continuación.

El elemento necesario para proceder a una verificación del voto por parte del votante es el recibo de votación, obtenido en el momento en el que el usuario emite su voto. Pero este no debe expresar el sentido del mismo pues de otra forma se convertiría en un justificante del sentido del voto, algo que se debe evitar para impedir la coacción sobre el votante. Este parece ser un problema de imposible solución, pero gracias a los investigadores ha sido resuelto de diversas formas. Todas ellas están dentro de la tendencia actual de resolver la justificada necesidad de disponer de procedimientos seguros y sencillos que permitan una auditoría de los procesos de VE, tanto por parte del usuario como de forma general. A estos los han venido a denominar sistemas de votación auditables de extremo a extremo E2E (End-to-End auditable o End-to-End voter verifiable).

En este sentido y desde el 2004 han ido apareciendo soluciones basadas en cifrado como:

* Scantegrity y Scantegrity II de un equipo en los que destacan David Chaum, Ronald L. Rivest y Peter Ryan [40] [41]
* Prêt à Voter de Peter Ryan [42] [43]
* ThreeBallot de  [Ronald L. Rivest](http://en.wikipedia.org/wiki/Ron_Rivest) [44]
* Scratch and Vote de Ben Adida [45]
* Bingo Voting de Jens-Matthias Bohli, Jörn Müller-Quade y Stefan Röhrich

Existen también soluciones sobre Internet:

* Adder de Aggelos Kiayias, Michael Korman y David Walluck [46]
* Helios de un equipo dirigido Ben Adida [47] [48]

No es objeto de este libro blanco entrar en el detalle de cada uno de estos sistemas ni mucho menos en una descripción de los métodos de cifrado utilizados para que el votante pueda verificar su voto una vez depositado. Lo que si tiene que quedar claro es que todos ellos permiten una auditoría del correcto funcionamiento del sistema y previenen contra la coacción al votante. Podemos denominar a este tipo de auditorías como indirectas, ya que no es necesario desplegar auditorías complejas y profundas de todos los elementos implicados, basta con verificar sus aspectos básicos como pueden ser el anonimato y el correcto recuento de los votos [49].

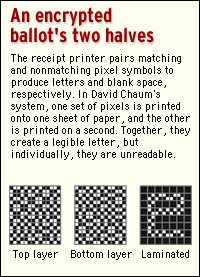


Figura 4 Cifrado gráfico del voto (Chaum)

Lo que si podemos garantizar es que estos diseños a día de hoy, finales del 2013, son los que más garantías ofrecen en una votación electrónica, ya sea con equipos de lectura óptica, DRE o votación telemática. Además los dos últimos, Helios y Adder, están basados en licencias de uso público tipo GNU-GPL. También es cierto que con este tipo de soluciones, existe la posibilidad de encontrarse con dificultades propias de las aplicaciones abiertas, pero en el caso de Helios podemos decir que lo hemos utilizado en varias ocasiones sin más dificultades que las propias de la puesta en marcha de una aplicación sobre un portal web [50].

Aun así, todos ellos han sido poco utilizados [48] e incluso han sido puestos en duda por algunos autores por problemas relacionados con el secreto del voto, similares a los del voto por correo. [51] [52]

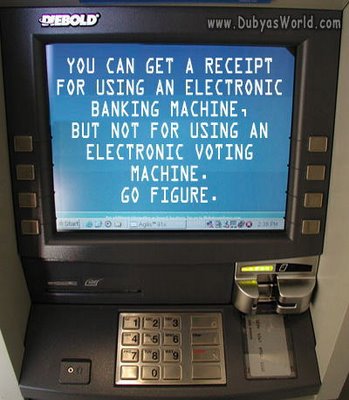


Figura Justificación del recibo de voto

# 7. Uso mundial del voto electrónico

## 7.1 Visión general

La mayor parte de los países en el mundo han considerado el uso del voto electrónico. De ellos una buena parte han realizado pruebas y algunos ya utilizan el voto electrónico de forma vinculante. En Europa, como ahora veremos, se han desarrollado diversos esquemas con pruebas en la mayor parte de los países. Fuera de Europa el uso del voto electrónico está ampliamente desarrollado en la mayoría de los estados de U.S.A. y en Brasil, Venezuela, seguidos de cerca por Méjico. Está siendo considerado en buena parte de los países de América Central y del Sur. Además tenemos a una parte de los antiguos países que formaron la Unión Soviética, India y Australia. Vamos a ver con más detalle las experiencias más destacadas en algunos de estos países.

**Suiza**, que recordemos está fuera de la Unión Europea, es un ejemplo a seguir por el desarrollo en la implantación del voto electrónico. En este país, dividido administrativamente en cantones, se llevan a cabo consultas de forma continua y era muy utilizado el voto por correo. Posteriormente en algunos de los cantores se pusieron en marcha pruebas de voto electrónico utilizando diversos métodos y durante varios años. Estudios posteriores determinaron su uso vinculante, sobre todo después del alto incremento en la participación que se produjo en los referéndums de 2003 y 2004 realizados en Anieres, Cologny y Carouge. Hoy la mayor parte de los ciudadanos suizos utilizan y confían en el voto electrónico y esto se debe a un adecuado diseño y una lenta implantación.

**Bélgica** fue el pionero del voto electrónico en Europa. Lo utilizaron en el cantón de Verlainer en 1991 con tarjeta magnética y lápiz óptico. En Octubre del 2000 ya el 42% de la población votó 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** ha llevado a cabo grandes pruebas en estas tecnologías incluyendo el voto por Internet y teléfono. La mayor de ellas se desarrolló en Junio de 2004 para las elecciones al parlamento europeo. Actualmente 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 qué se está votando. La empresa que fabrica la urna (Nepad) garantizó que corregiría los errores. Esta misma máquina con pequeñas variantes se está utilizando en pruebas en Alemania y Francia. También en este país se utilizó un sistema de votación telemático que permite la auditoría E2E, denominado RIES, que permitió la participación de 20.000 votantes ausentes en las elecciones a su parlamento en el 2006.

En **Inglaterra** se han desarrollado pruebas a nivel municipal desde el 2000. En Junio de 2004 se hizo 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, lo cual no significa que por el camino no aparezcan problemas como lo ocurrido en los comicios municipales celebrados en Mayo de 2007 en los que se perdieron una parte de los votos. Un estudio posterior critica la falta de un sistema lo suficientemente riguroso de auditoría que asegure que tanto el hardware como el software que se utiliza están libre de vulnerabilidades, de lo cual ya hemos hablado anteriormente.

**Escocia** que un caso similar al anterior. Además dispone de uno de los sistemas de participación ciudadana (e-petitions) para su parlamento más elaborado, analizado y cuidado de Europa [53].

**Irlanda** desde el año 2000 ha llevado 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.

**Alemania** comenzó sus primeras pruebas de voto electrónico en 1999 pero en ámbitos no políticos y ha elaborado una documentación precisa sobre los requisitos que deben de cumplir los equipos involucrados. Posteriormente, en septiembre de 2005, se 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** estableció en Julio de 2003 un plan para el voto electrónico. 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 en el 2003 utilizó Internet para elecciones para el Consejo Superior de Franceses en el Extranjero (CSFE), pero sin conseguir incrementar la participación. También se ha utilizado 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 las elecciones presidenciales del 2007 también se utilizaron urnas electrónicas por parte de 1,5 millones de personas de un total de 44,5 millones del censo. Se registraron problemas sobre todo con los votantes de mayor edad.

**Italia**, de forma muy similar a Francia, también utilizó el voto electrónico no vinculante y a pequeña escala en colegios electorales.

**Estonia** es un país pionero en el uso vinculante y flexible del voto por Internet y lo analizaremos en el apartado correspondiente.

Los **Estados Unidos de América** son un caso único en el mundo debido a la gran complejidad de su sistema electoral, en el que cada Estado e incluso cada Condado determinan la forma y los recursos electorales a utilizar. En las elecciones presidenciales de noviembre de 2000, casi el 70% de los votantes utilizó la vía electrónica para emitir su voto, contando con anticuados mecanismos como la tarjeta perforada, aunque también se utilizó el voto con lectura óptica y sistemas DRE. En esta ocasión las irregularidades fueron muy importantes, sobre todo en el Estado de Florida debido a problemas con la lectura automática de las papeletas perforadas [54]. En los comicios nacionales de 2004 en los EE.UU. la mayor parte de los votantes emplearon sistemas automatizados: el 13,7% de los ciudadanos votaron con tarjetas perforadas; el 14% empleó sistemas similares a la manivela de hace más de 100 años; el 34,9% sufragaron en equipos de lectura óptica y el 29,3% empleó para votar equipos desarrollados bajo el concepto de los DRE. El mapa actual es sumamente complejo y disperso [55] aunque predomina el voto con DRE y VVPAT. 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 destacables de estos sistemas es el que tuvo lugar en el estado de Florida, donde la falta de normativa y control, unido a una tecnología obsoleta (tarjeta perforada), propició que muchos votantes no pudieran saber con certeza qué opción era la que habían marcado.



Figura 6 Voto en papel perforado (USA)

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 [56]. Posteriormente se fueron sumando más verificaciones negativas hasta el punto 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”.

En los EE.UU. existe un debate muy enriquecedor sobre el uso de la tecnología en los procesos electorales. Desde finales del 2006 funciona en la Universidad Johns Hopkins un centro de estudio destinado a incrementar la confianza en las tecnologías del voto electrónico [57]. 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 esta no es una propuesta privada. La iniciativa denominada ACCURATE (preciso), 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 EE.UU. [58].

Con el respaldo de la Ley denominada Ayude a América a Votar (HAVA), promulgada en el año 2002 [59], los gobiernos municipales y locales de EEUU están debatiendo sobre la conveniencia de aumentar la tecnología en los próximos comicios.

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, ha analizado las máquinas y la programación de votación electrónica, incluidos los mecanismos de cifrado que se utilizan para garantizar que los electores mantengan su privacidad, así como, los métodos utilizados para verificar que los ordenadores totalicen con precisión todos los votos legítimos [56] ; otros miembros del equipo se encargaron de los aspectos legales y de las políticas públicas que han 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, establecer procesos permanentes de análisis, facilitar los estudios independientes, ejecutar auditorias 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 comprobar que cada sistema registra los votos de manera adecuada, impedir que el código fuente de los equipos pueda ser modificado, exigir una revisión de las pantallas en todos 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. Este último aspecto es hoy en día considerado como la solución con mayores garantías, como ya hemos expuesto. Claro que todo esto puede hacer que el proceso automatizado se convierta en más complejo que el manual, ya que requerirá la verificación manual sobre el proceso automatizado, es decir dos procesos en uno, y por tanto se puede convertir en más complejo, lento y caro. Cabe destacar que el profesor Rubin publicó en el 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 las agencias responsables no toman las medidas necesarias para hacerlas seguras. Si usted vive en U.S.A. no necesita imaginárselo. Esta es la realidad del voto electrónico en este país”.

**Canadá** sigue la estela de los EE.UU. en esta materia. Aunque a nivel federal no se utiliza el voto electrónico, sí se hace en las municipales y locales en algunas ciudades desde 1990. Carece de estándares propios pero utiliza los que su vecino americano va creando. Cada provincia escoge su tecnología y tiene sus propias normas.

**Méjico**, al igual que otros países, depende de los Institutos o Comisiones Electorales de los Estados para la definición del uso de las diversas tecnologías para el VE. Los Estados de Coahuila, Distrito Federal, San Luis de Potosí y Jalisco tienen urnas electrónicas que ya han sido utilizadas en algunos procesos electorales. El pionero fue Coahuila que ha desarrollado su propia DRE.



Figura 7 Urna de Coahuila (Méjico)

En este caso cabe destacar que los desarrollos son propios y los equipos han sido auditados en algún momento [38]. Estas 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 costes.



Figura 8 Urna de Jalisco (Méjico)

**Australia** empezó a utilizar máquinas de voto electrónico en las elecciones parlamentarias de Octubre de 2001, que fueron usadas por más de 16.000 votantes. Ya en 2006 el gobierno del Estado de Victoria introdujo en las elecciones estatales una prueba general con voto electrónico. Posteriormente la Comisión Electoral Australiana ha decidido introducir en 29 localidades el voto electrónico para que puedan utilizarlo 300.000 discapacitados visuales. 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 está siendo llevado a cabo lentamente y con acierto. Nótese las grandes extensiones de territorio en este país. Es otro modelo a seguir.

## 7.2 Experiencias más relevantes y sus debilidades: Venezuela, Brasil y la India

**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 problema por el procedimiento de verificación del votante mediante lectura de huella dactilar con una máquina denominada “captahuellas” o “cazahuellas” [7], ya que se utilizan las mencionadas máquinas para verificar la identidad de los votantes mediante enlaces satelitales que permiten verificar en “tiempo real” este extremo y existió la sospecha de que eran utilizadas para hacer listas ordenadas de los votantes. Se plantearon problemas muy interesantes debido a la sospecha de que se pudieran relacionarse 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 2005 se retiraron cautelarmente, pero volvieron a ser utilizadas en Diciembre de 2006, argumentando que se había roto la secuencialidad utilizando un procedimiento de recolocado seudoaleatorio de los votos en grupos de 10. El despliegue tecnológico en las elecciones de este país es uno de los más complejos, ya que además de las urnas electrónicas que emiten el voto en papel que posteriormente se introduce en una urna convencional (ver figura 9) para proceder, en algún caso determinado por sorteo, a su recuento manual (verificación por papel). En cualquier caso el recuento resulta lento y complejo debido al diseño del mismo y a la necesidad de realizar la auditoria manual en alguna de las urnas. El proceso ha sido refinado en sucesivas ocasiones mediante observaciones externas.

Figura Segundo paso: voto clásico

El caso venezolano es un caso muy singular por las circunstancias que concurren. El despliegue de infraestructuras de voto electrónico se produjo en un contexto de fuerte controversia política que nunca es el mejor contexto, en una sociedad muy polarizada y una elevada dosis de desconfianza institucional fundamentada en factores objetivos. Los resultados del referéndum revocatorio de 2004 fueron duramente contestados y la oposición, dado el tipo de resultados que se produjeron, defendió la tesis de que se había producido una manipulación generalizada sobre el hardware de las urnas electrónicas, en particular las memorias flash que almacenaban los datos de urnas de distritos muy significativos que indujeron resultados favorables para Hugo Chávez. Los expertos adujeron, en función de los resultados de participación y la secuenciación de los votos, que muchas de dichas memorias habían sido sustituidas por otras con resultados prefabricados.



Figura Tipos de DRE en Venezuela (Smartmatic)

Conviene que se sepa que el papel jugado por la Fundación Carter fue demoledor. Los expertos desplegados por dicha fundación de ningún modo estaban cualificados para valorar las infraestructuras de voto electrónico y los distintos analistas coinciden en señalar que los resultados de su observación fueron poco esclarecedores. Los protocolos de despliegue de dichas infraestructuras fueron muy deficientes y sobre todo opacos y, para dejar todo dicho, la oposición tampoco adoptó las cautelas que el caso exigía, siguiendo todos los procesos de información, intervención y auditoría que son exigibles. Únicamente se admitió a un grupo de expertos denominados GST (Grupo de Seguimiento Técnico) que elaboraba informes que no eran públicos ni vinculantes.

La opinión del OVE, que declinó su presencia como observador en las elecciones municipales venezolanas del primer trimestre de 2005, es una opinión reservada y subjetiva no refrendada por elementos probatorios, es que se dan dudas razonables para poner en entredicho la intencionalidad de la arquitectura física y lógica de las infraestructuras desplegadas. El OVE declinó la petición de la Presidenta del Consejo Nacional Electoral Venezolano (CNE) porque no se nos proporcionó la información que el OVE prescribió como imperativa para realizar la observación y tampoco se nos garantizaban las acreditaciones reclamadas, que incluían un nivel de acceso suficiente a los centros de totalización de datos y a los centros logísticos que operaban con las urnas electrónicas. Se acudió al sempiterno argumento de los derechos de propiedad intelectual de la empresa proveedora, para no aportar la arquitectura lógica de los sistemas que soportaban el cómputo y almacenamiento de los votos en las urnas electrónicas, ni el código fuente correspondiente a las distintas etapas del proceso, desde la identificación de electores hasta el recuento, pasando por la captura del voto. Es por ello que este sistema no ha sido nunca auditado de forma pública, al no haber permitido a los expertos el acceso físico a esta urna ni a los detalles técnicos, siendo por tanto una excepción en el mundo.

En las últimas elecciones del 2013 se incluyó la lectura de las huellas dactilares para la autentificación del votante en la propia red de votación suscitando aún mayor controversia. Además el ciudadano deposita el voto en papel generado en la DRE en una urna convencional, con lo que puede escamotearse el voto y producir una cadena de coacción también denominado “voto controlado en cadena”.

**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, lo cual está plenamente justificado por el número de electores y la complicada orografía del país. La votación se lleva a cabo a través de una especie de cajero automático con una pantalla, en el 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 o para ser enviado por enlace satelital al punto habilitado más cercano. La urna electrónica fue el único método de votación en las elecciones a Presidente de la República en octubre de 2002 y fue empleado con éxito por 115 millones de votantes.

Este es otro caso especial ya que debido a su complicada orográfica y al historial de manipulaciones y fraudes electorales, forzaron la aparición del voto electrónico como única salida viable. Para darnos una idea, ya en las elecciones municipales de Octubre del 2000 votaron electrónicamente 109 millones de ciudadanos. Además se dio la oportunidad de votar a los analfabetos (20 % de la población).



Figura DRE de Brasil con lector de huellas

El sistema utilizado es una urna electrónica con un teclado de desarrollo propio. La experiencia en este país demuestra que el voto electrónico ha reducido de forma muy importante el voto nulo, debido a que se vota simultáneamente para tres niveles de representación administrativa y esto ha incrementado la participación. En cualquier caso en el año 2012 el profesor Aranha y su equipo de la Universidad de Brasilia consiguieron *hackear* la urna electrónica de su país [33]. Si a esto se le añade que en enero de este año, 2013, un hacker demostró en directo en Río de Janeiro como acceder a la intranet de la red del Tribunal Electoral de esta ciudad y manipular los resultados sin ser detectado [60]. Así podemos establecer que el sistema necesita ser mejorado para generar la confianza necesaria en el electorado. A pesar de todo este país es ejemplo de uso adecuado del V.E. ya que el voto convencional generaba aun más inconvenientes que esté basado en tecnología.



Figura DRE Brasileña

**India** es otro 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 electores con la multitud de partidos políticos que se presentan?). Ya en el año 2.004 se distribuyeron por encima de un millón de EVM (electronic voting machines) que suministraron 2 empresas del propio país, con un diseño sobrio, un coste de fabricación reducido, pero de manejo poco claro. La puesta en marcha del voto electrónico en todo el país se hizo de forma paulatina y comenzó en 1989. De esta forma se fue aprovechando la experiencia para aumentar año a año el número de máquinas.



Figura Aspecto de la votación en la India

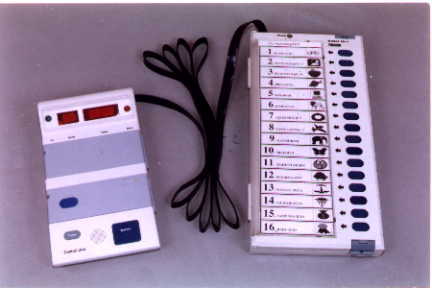


Figura DRE de la India

Este podría ser 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 debido al elevadísimo número de electores y de opciones políticas, a la arcaica red de comunicaciones y a la enorme extensión del país. Pero en el 2010 el profesor Halderman de la Universidad de Harvard demuestra que el EVM no garantiza la imposibilidad de manipulaciones y hace una demostración de cómo modificar los resultados [5]. 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, asegurando que el verdadero propósito de unas elecciones no es que los ganadores asuman que han ganado, sino convencer a los perdedores que han perdido. Por todo ello el proceso ha sido puesto en duda e iniciado un período de revisión profunda.



Figura El Dr. Halderman y sus colaboradores

Una vez más es necesario determinar que es preferible para el electorado, un proceso clásico que puede ser igualmente manipulado y al que se le añaden tiempos de recuento muy largos y por tanto sospechas de manipulación, o bien, este tipo de solución que se caracteriza por un rápido resultado, que aunque mejorable, permite el sufragio de todos. Compleja decisión en la que si tenemos en cuenta que ninguna de las dos es perfecta, hay que decidirse por aquella que menos lesiona los derechos democráticos.

## 7.3 Iniciativas europeas

La Unión Europea desarrolló un proyecto denominado EU CyberVote Project 34 durante los años 2002 y 2003. El objetivo era verificar las garantías de privacidad y seguridad en una votación en línea sobre Internet utilizando terminales fijos y móviles. Fue desarrollado por las empresas más reconocidas de telefonía y tecnología y muchos suponen que no podría haber sido de otra forma. Las conclusiones son que el prototipo diseñado por CyberVote 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 de Internet.

Por otra parte el Consejo de Europa (CoE) constituyó en Noviembre de 2002 un grupo de expertos denominados IP1-S-EE [61] para fijar estándares para el voto electrónico (*e-enable voting*). Posteriormente se constituyeron dos subgrupos, uno de aspectos legales y operacionales y 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 [62]. Estas 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 de ser un canal adicional y opcional de voto, nunca único.

La principal iniciativa dentro de la Unión Europea en relación al desarrollo de los denominados sistemas de voto electrónico viene reflejada en esta recomendación Rec(2004)11 . Dicha recomendación, propone un conjunto de medidas a adoptar por aquellos países miembros que decidan implantar métodos de sufragio alternativos a los existentes en la actualidad. Curiosamente buena parte de las experiencias europeas puestas en marcha posteriormente no han seguido estas recomendaciones [39].

Los objetivos de la recomendación y el conjunto de normas que la componen son:

* Salvaguarda de los principios consignados en el código de buenas prácticas electorales aprobado en la Resolución 1320(2003) principios que dictan que un sufragio deberá ser de carácter universal, único, libre, secreto y directo.
* Asegurar la confianza de los ciudadanos en los sistemas alternativos de voto electrónico.
* Fomentar la interoperabilidad entre diferentes sistemas de voto electrónico.

La recomendación atañe a la celebración de aquellos procesos electorales o referéndums en el seno de la Unión Europea si bien cada estado miembro podrá adaptar, en función de su regulación específica, la aplicación de la recomendación.

Su desarrollo se basa en los principios de carácter legal, operativo y técnico que deben regir en la celebración, ya sea de elecciones o referéndums, en los estados miembros y en la propia institución europea.

En relación con los principios de sufragio universal y único, los sistemas para la emisión del voto han de ser accesibles para el conjunto de la ciudadanía y en especial para aquellos colectivos que presenten algún tipo de discapacidad. Asimismo deberán existir procedimientos que aseguren la unicidad del voto emitido por cada persona autorizada a hacerlo.

En lo que respecta a los principios de sufragio libre y secreto, las autoridades competentes velarán por la celebración de elecciones que respeten los períodos de reflexión previos establecidos así como la ausencia de elementos condicionantes durante el ejercicio electoral. Del mismo modo el elector deberá ser informado una vez haya completado el proceso de emisión de su voto, así como una vez se haya completado el escrutinio de los votos emitidos. Bajo ninguna circunstancia será posible alterar un voto una vez haya sido emitido. Con el fin de asegurar la privacidad del voto los sistemas y procedimientos empleados garantizarán la imposibilidad de asociar los votos emitidos con las personas que los emitieron, ya sea durante el proceso electoral o una vez haya finalizado el mismo.

## 7.4 Iniciativas y experiencias españolas

España también ha desarrollado pruebas de voto electrónico, pero ninguna de ellas ha sido vinculante ya que no lo permite la legislación electoral. Incluso en Febrero de 2005 se desarrolló la primera prueba de voto electrónico por Internet que será analizada a continuación.

Tenemos toda una historia con un sabor agridulce. En este sentido hay que reconocer que los fracasos han sido diluidos con una política poco transparente que en nada ayuda a cimentar adecuadamente los avances de este país en esta materia, máxime cuando tenemos empresas y desarrollos de primer nivel en este sector.

Destacaríamos las iniciativas del ayuntamiento de Jun (Granada) y de los ayuntamientos de Madrid y Barcelona. Las experiencias de las elecciones sindicales en la Policía Nacional y la prueba no vinculante sobre el referéndum sobre la Constitución Europea de febrero de 2005.

Si hay alguien al que se le puede considerar pionero en el intento de poner en marcha el VE en España es al alcalde de Jun, José Antonio Rodríguez, que ya en el año 2001 inicio una experiencia que la prensa vino a denominar “teledemocracia” y “ciberdemocracia” [63].

En junio de 2004 el Ayuntamiento de Madrid convocó a los cerca de 140.000 habitantes del distrito centro de Madrid para expresar su opinión sobre cuestiones relacionadas con sus competencias, con la ayuda tecnológica de la empresas Scytl y H.P. [64]. En este caso hubo destacados informes [65] en los que se pide prudencia a la hora de poner en marcha procesos de votación electrónica.

En mayo de 2010 se puso en marcha una experiencia en Barcelona para decidir qué hacer con la Diagonal. Esta fue una votación telemática a través de un portal web, con un censo cercano al millón y medio de ciudadanos durante 4 días. Posteriormente también se admitió el voto presencial. Este asunto acabó con la dimisión del primer teniente de alcalde del Ayuntamiento por errores en la puesta en marcha y desarrollo del VE en esta consulta [66]. Las empresas implicadas (Indra y Scytl) tuvieron que justificar los problemas de todo tipo que aparecieron durante esos días.

De estas pruebas se pasó a experiencias vinculantes aunque en ámbitos de un nivel inferior al electoral ya que jurídicamente y a día de hoy no son posibles. Este fue el caso de las elecciones sindicales de junio del 2011 en la Policía Nacional que también acabaron con polémica. En este caso fue Telefónica la implicada y la prensa lo calificó de “pucherazo” [67]. En cualquier caso tuvieron que repetirse posteriormente y se solicitó una auditoría, que como ya hemos justificado poco puede aclarar en este ámbito.

Por último nos queda hablar de la experiencia no vinculante de voto telemático en febrero de 2005 que llevó a cabo la empresa Indra que resultó ser un fracaso técnico y de participación. Lo analizaremos en el siguiente apartado.

## 7.5 Experiencias de voto telemático o remoto

Todas las experiencias de este tipo que han sido realizadas con valor vinculante se han desarrollado en contadas ocasiones.

En **Estonia** en las elecciones municipales del 2005 y del 2009 y en las presidenciales del 2007 y del 2011. Ya en el otoño del 2005 se realizó una prueba piloto avanzada en unas elecciones locales, utilizando *smart cards* con firma electrónica. Posteriormente en las elecciones parlamentarias del 2007, 30.275 personas votaron por Internet (3,5% de la población) [68]. En cualquier caso este 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 infraestructuras PKI. En este caso el voto remoto no era el único admitido e incluso podía votarse varias veces teniendo validez el último emitido que podía ser por el método tradicional que también estaba habilitado y es lo que se denomina multicanal. Se llevó a cabo mediante una tarjeta de identidad y una infraestructura de clave pública. En el 2011 la participación por medio del voto telemático fue de poco más del 15%.

Un ejemplo de uso estudiado y que se ha ganado la confianza del ciudadano es el ya comentado de **Suiza** que lo utiliza en los referéndums desarrollados en algunos cantones de forma habitual con objeto de conocer la opinión del ciudadano y elegir propuestas.

En **Estados Unidos** que se han utilizado en las elecciones en Alaska y en la experiencia con el personal del ejército fuera de su país denominado SERVE. El ejército de Estados Unidos desaconsejó el sistema por deficiencias severas en la arquitectura lógica y los bajos niveles de seguridad. La exposición a ataques de toda la arquitectura lógica fue muy censurada y posteriormente contestada por los expertos del Pentágono. El sistema esperaba 100.000 votos en una primera fase para llegar a 6 millones, con un coste estimado de 24 millones de dólares. Después de un análisis de su seguridad por parte de David Jefferson, en el que se ponían en entredicho muchos de los aspectos de seguridad del sistema, el proyecto se detuvo [69].

**España** también ha desarrollado pruebas de voto telemático, pero todas ellas no vinculantes ya que no lo permite la legislación electoral. En Febrero de 2005 se desarrolló la primera prueba de voto electrónico por Internet que resultó ser un fracaso técnico y de participación. La prueba se desarrolló con la mediación de Indra y sobre un censo de 2 millones de votantes y utilizando ordenadores ubicados en dependencias cedidas por los municipios, uno por provincia. Los censados podían dirigirse a estos lugares y usar el ordenador para votar de forma paralela y no vinculante en la consulta sobre la Constitución Europea o recoger un código para votar desde su domicilio. La participación no llegó a los 11.000 votantes y por si fuera poco el OVE emitió un duro informe sobre las irregularidades técnicas detectadas [70].

También en España se ha desarrollado Votescript, un producto completo de voto telemático seguro realizado por el Dr. Carracedo y su equipo. [8] “Incluye la realización del análisis, la definición y la implementación de un sistema capaz de soportar los diferentes pasos y elementos existentes en un proceso de votación telemática, abarcando desde el proceso de emisión del voto hasta el de recuento y posterior verificación de los resultados.”

Existen otras iniciativas mundiales de voto telemático que pueden igualmente ser consideradas, ya que reúnen las condiciones básicas y necesarias. Este es el ejemplo de Helios del Dr. Adida y su equipo. [47]

La inexistencia de datos añade problemas de seguridad al voto remoto, un voto que necesita reforzar todas las cautelas en los centros de cómputo y donde la arquitectura lógica desempeña un papel crucial. Al voto remoto se le han añadido numerosas pruebas piloto utilizando la telefonía móvil como soporte. En Europa se han hecho numerosas pruebas piloto utilizando la telefonía de segunda generación y de 3G. En opinión del OVE son pruebas inapropiadas en su formulación y en su ejecución. No debieron producirse, ni siquiera en grado de hipótesis. No cumplen los requisitos legales que son propios de una consulta electoral. Han constituido pasatiempos que han llegado a experimentarse al amparo del nivel de desinformación de las autoridades electorales de cada país y de intereses ajenos al derecho electoral

En definitiva es añadir a todas las desconfianzas que ya de por sí tienen las infraestructuras presenciales del VE, las propias de Internet. En este sentido la literatura que pone en duda la seguridad del voto telemático es muy amplia. [23]

## 7.6 Conclusiones de las experiencias mundiales

Podemos sacar varias:

* 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.
* Se producen cambios de opinión de forma continua en este tema, lo que demuestra que no ha sido diseñado ni puesto en marcha de forma adecuada.
* 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, los jurídicos, los legisladores, políticos y al público en general.

Es imprescindible generar CONFIANZA en los ciudadanos y esta no se consigue sin transparencia, formación y debate público.

# 8. Empresas y productos

En este país tenemos dos de las empresas más destacadas en el VE en el mundo: Scytl e Indra.

**Scytl Secure Electronic Voting** [71] es una empresa líder en el desarrollo de soluciones seguras para el voto electrónico remoto. Fundada en junio 2001 como división de un grupo de investigación de la Universidad Autónoma de Barcelona, cuenta con más de 10 años de experiencia en investigación y desarrollo en el sector del software para el voto telemático.



Figura La aplicación Pnyx de Scytl

Desde su inicio, Scytl ha recibido numerosos premios a la innovación tanto en España como en Europa. En Septiembre 2004, Scytl fue galardonada con uno de los 20 IST Prize Winners que otorga la Comisión Europea a las mejores empresas tecnológicas europeas, el galardón más prestigioso para una compañía tecnológica en Europa.

Esta empresa ha llevado a cabo múltiples proyectos de voto y consulta electrónica para diversas administraciones y empresas, tanto a nivel nacional como internacional, como los proyectos EPC 2003 (Elecciones al Parlamento de Cataluña), Neuchâtel en Suiza o Madrid Participa, todos ellos llevados a cabo con el sistema Pnyx para realizar votaciones electrónicas remotas.

En la actualidad, Scytl está participada por WebCapital SCR y Spinnaker SCR, dos fondos de capital de riesgo gestionados por el Grupo Financiero Riva y García.

Los productos de Scytl están orientados a ofrecer soluciones seguras y sencillas para todo tipo de votaciones electrónicas, desde procesos electorales normales hasta juntas de accionistas y todo ello con las garantías técnicas que aseguran el mismo nivel de seguridad que los procesos habituales. Aun así se ha visto envuelta en procesos que han finalizado en polémica y ya comentados anteriormente. En cualquier caso las soluciones están sujetas a las limitaciones de seguridad propias de Internet.

Scytl ha estado trabajando en los últimos años en el concepto de e-democracia, una idea que trata de potenciar la participación de la ciudadanía en las cuestiones públicas permitiendo obtener de forma rápida y automatizada la opinión de los ciudadanos.

Uno de los desarrollos estrella es **Pnyx**, que según la propia empresa es “una familia de productos que permiten realizar por medios electrónicos todo tipo de procesos electorales (elecciones públicas y sindicales, referéndums , consultas ciudadanas, votaciones en Juntas Generales de Accionistas, etc.) con las mismas garantías de seguridad, privacidad y confiabilidad que los procesos electorales tradicionales basados en papel, y con las ventajas que ofrecen los sistemas electrónicos: accesibilidad, flexibilidad y rapidez en el recuento de votos”.

Se trata de una herramienta accesible desde cualquier dispositivo conectado a Internet con un navegador que soporte Java.

Soporta diversos mecanismos de identificación como login y password (con certificación digital avanzada) y firma electrónica reconocida, con objeto de asegurar la identificación del elector y la privacidad de los participantes respecto a la opinión emitida.

Otros productos de la empresa son:

**Pnyx.government** es la aplicación de Scytl orientada a la Administración Pública (municipios, gobierno central, gobiernos autonómicos, diputaciones provinciales, etc.).

[**Pnyx.Labour**](http://www.scytl.com/esp/pnyx_labour.htm) es la plataforma de Scytl para elecciones sindicales de grandes empresas y a órganos de gobierno de colegios profesionales, universidades, cajas de ahorros, etc.

[**Pnyx.Corporate**](http://www.scytl.com/esp/pnyx_corporate.htm)es una aplicación orientada al voto y delegación electrónicos en Juntas Generales de Accionistas.

**Pnyx.DRE** es la solución de Scytl para dotar de seguridad a cualquier terminal de voto electrónico presencial, de forma que sea totalmente confiable y auditable. [Pnyx.DRE](http://www.scytl.com/esp/pnyx_dre.htm) permite, mediante un simple módulo externo conectado al terminal de voto electrónico, garantizar la integridad del proceso. En este caso se da la opción a los votantes de verificar su voto antes de ser emitido.

Para llevar a cabo el proceso de consulta con estos sistemas se deben de dar varios pasos previos:

En primer término, se ha de poner en conocimiento de los electores implicados la utilización del nuevo proceso y las instrucciones que se deben seguir para completar la votación.

Se debe realizar también un proceso de registro de participantes ya que hasta la implantación del DNI electrónico, la administración debe utilizar otros mecanismos para la identificación del elector. Estos suelen ser o bien la distribución de tarjetas electrónicas electorales entregadas mostrando el DNI en alguna oficina habilitada al efecto o por correo (en este caso se debe suministrar algún dato personal en el momento de la votación para evitar fraudes); o bien mediante el uso directo de datos personales y *passwords*.

De este modo, los ciudadanos pueden participar de forma sencilla desde cualquier PC con acceso a Internet, y a cambio obtienen un recibo que les permite comprobar (con absoluta fiabilidad) que su voto ha llegado al comité, el cual lo tendrá en cuenta en el recuento final. Se reúne el comité, quien abre la urna electrónica y efectúa el procesamiento de los votos emitidos. Se genera un listado con los recibos de voto utilizados para obtener los resultados, que se publican para que cualquier ciudadano pueda comprobar que su voto llegó al comité y fue tenido en cuenta. Es evidente que esta solución no evita la coacción sobre el votante.

**Indra** [72]es una empresa líder en la organización de procesos electorales. Más de 350 procesos en 22 países. Dispone de su propia DRE denominada Point&Vote y de una solución de voto por Internet, NetVote. En cualquier caso su especialidad es la organización de procesos electorales y concretamente la gestión del recuento de votos. Como en todo los casos tiene ejemplos de éxito y de fracasos, sobre todo en los relacionados con el voto por Internet, como no podía ser menos.



Figura DRE de Indra

**Smartmatic** [73]esta es una empresa de características especiales. El propietario mayoritario es de origen español, Antonio Múgica, y en 2006 compró otra importante empresa estadounidense del sector: Sequoia Voting Systems, Inc. Por lo que fue investigado por las autoridades americanas. Ha estado presente en prácticamente todas las elecciones de Venezuela desde el 2004, siendo seleccionada de forma directa sin concurso público. Se ha encontrado envuelta en polémicas y controversias continuas, tanto dentro del país como en los medios americanos. Las últimas elecciones en las que se utilizaron sus equipos fueron en las municipales venezolanas el 8 de diciembre de 2013. Sus equipos han ido evolucionando y han sido auditados por expertos del GST, pero no así el proceso global ni mucho menos por parte del ciudadano. Los equipos cumplen con los requisitos técnicos esenciales pero dos dudas siguen presentes en la organización de sus procesos: la correlación que de forma exterior al sistema se puede obtener entre el orden de votación y la relación final de votos emitidos que genera el equipo al cierre del sistema y, el establecimiento de cadenas de coacción externa al pasar el voto en papel generado por la DRE por manos del votante.

**Diebold** [74], tiene una larga experiencia en procesos electorales usando maquinas automatizadas. Estados Unidos lleva años utilizando su tecnología para el recuento de votos y muchos estados confían ya en las máquinas AccuVote TS para realizar las votaciones. Dispone de un denso historial de experiencias con fracasos y éxitos.

Una de las últimas experiencias a tuvo lugar este año (2005) en el estado de Ohio y ha sido calificada como un rotundo éxito. Se instalaron 15.000 máquinas de votación AccuVote TSX en 44 condados del Estado. Votaron cerca de un millón de personas en 4.100 colegios electorales. Para ayudar en los procesos electorales, se impartieron clases de formación para 20.000 ciudadanos que colaboraron para que el proceso se llevara a cabo con total normalidad. Además, otros 400 técnicos estaban preparados para solucionar cualquier problema que pudiera surgir. Este es el precio de la puesta en marcha de este tipo de infraestructuras.



Figura Dos tipos de DRE de Diebold, con VVPAT (sin acceso) y con lector de identidad

Alaska, Georgia, Arizona, Virginia y Kansas han utilizado también en alguna ocasión los sistemas de voto electrónico que oferta Diebold.

A pesar de todo ello la empresa se ha visto envuelta en varios escándalos por su baja seguridad en la encriptación y en el manejo de la información y está revisando todo su software. De hecho el denominado “caso Diebold” ha sido el más importante ejemplo de baja confiabilidad detectada en un sistema de votación electrónica. Es más, debido a él, se desarrolló el más importante debate sobre este tema, desarrollándose estudios más serios y profundos y desencadenándose una serie de comunicaciones entre los expertos y la empresa que obligaron a esta a reconocer determinadas debilidades en su sistema y sacar públicamente a concurso las mejoras para recuperar la confianza del público. Todo ello a pesar de que sus máquinas cumplían con los estándares VSS (Voluntary Voting Systems Standards) y estaban certificadas. Los riesgos en la seguridad del sistema Accuvote TS fueron denunciadas inicialmente por el profesor Rubin de la Universidad Jhons Hopkins en Junio del 2003, contestadas por la empresa y finalmente se hizo un informe por parte del propio estado de Maryland.

# 9. Estándares

El mayor esfuerzo por la estandarización de los sistemas de voto electrónico, se ha desarrollado a raíz del mayor fracaso en unas elecciones democráticas, nos estamos refiriendo a las elecciones presidenciales de los Estados Unidos en el 2000. Por esa razón se creó HAVA que es una iniciativa federal para promulgar estándares para el registro de votantes y para los sistemas electorales basados en tecnología. Sus esfuerzos han sido muy importantes y en muchos aspectos son pioneros en la estandarización y certificación de los sistemas de voto electrónico pero sus decisiones no son vinculantes ya que cada estado tiene sus propias leyes electorales e independencia en los procesos. En cualquier caso está presente en todas las recomendaciones y esfuerzos para la normalización y comprobación de estas tecnologías y es una referencia obligada, aunque muchos aspectos no se pueden extrapolar a nuestro entorno.

El desarrollo de estándares se ha realizado los Estados Unidos de América a través de la publicación de los VSS (Voluntary Voting Systems Standards) de la FEC (Federal Election Comisión), que han sido adoptados por muchos de los estados. Estos estándares voluntarios han sido pensados para los sistemas DRE, para los de exploración óptica (OCR) y para los lectores de tarjetas perforadas.

Con el fin de completar el proceso, la NASED (National Association of State Election Directors) (Asociación Nacional de directores estatales de elecciones) ha seleccionado a una autoridad de comprobación y prueba (ITA) para verificar y certificar que los sistemas de voto cumplen con los VSS. Para ello se realizan pruebas del hardware y del software de los equipos y se guardan las distintas versiones, con objeto de proceder a su comparación posterior.

Para este proceso se creó un comité técnico compuesto por 15 miembros con experiencia en estándares tecnológicos presididos por el responsable del NIST (National Institute of Standars and Technology). A pesar de este esfuerzo, los resultados han sido muy criticados por los expertos ya que su nivel de verificación no es tan alto como recomiendan los grandes institutos de normalización americanos y mundiales (ANSI e ISO). Debido a ello algunas máquinas certificadas por NASED conforme a los VSS dieron serios problemas en pruebas reales, por ejemplo el caso Diebold ya comentado. Es por ello que la EAC (Comisión de Asistencia a las Elecciones Americanas) ha promovido la creación de un nuevo comité para el desarrollo de las líneas básicas técnicas para el voto que reemplazarán a las VSS y contarán con la presencia de miembros de la ANSI, de la NASED y de la IEEE que ya ha desarrollado su propio estándar (SCC 38).

A nivel europeo el principal avance ha sido la recomendación 11 del 2004 del Consejo de Ministros (30 de Septiembre del 2004) sobre los aspectos legales, operacionales y técnicos del voto electrónico. Esta establece los estándares a esos tres niveles y recomienda que por parte de los estados miembros se desarrolle un proceso de certificación para cada uno de los componentes involucrados y que para evitar duplicidad de esfuerzos debería realizarse a través de forums para la cooperación en la acreditación, tanto a nivel Europeo como Mundial.

Podemos deducir que a pesar de los errores, lo importante es comenzar a desarrollar una normativa que permita verificar y certificar los diversos equipos involucrados en el voto electrónico, contando para ello con la mayor parte posible de expertos y manteniendo el proceso abierto y en continua mejora. Los estándares son esenciales para garantizar la seguridad en los equipos porque especifican los parámetros que pueden ser medidos con el objeto de reducir los riesgos de un mal funcionamiento o de una manipulación. En definitiva ayudan a buscar las vulnerabilidades y a mejorar los diseños para evitar riesgos. Sin duda estas mejoras en el diseño, tanto del *hard* como del *soft*, afectarán al precio final del equipo pero son irrenunciables. Además esto obligaría a certificar con una caducidad para forzar la revisión y mejora continua en los sistemas por parte de los fabricantes que tendrían que actualizar sus diseños para evitar nuevos riesgos.

Por último, expresar la opinión de algunos que consideran que los procesos para certificar y controlar estas máquinas nunca podrán garantizar la seguridad plena del voto electrónico, pues a diferencia de cualquier otro sistema, el secreto de la información debe ser pleno, tanto desde fuera como desde dentro, ya que nadie puede valorarlo internamente mientras está en marcha pues la trazabilidad del voto debe de ser imposible para evitar la pérdida del anonimato.

# 10. Propuestas y recomendaciones

Es curioso constatar que en este punto todo el mundo coincide, independientemente del país y del tipo de experiencias que hayan llevado a cabo. En general, el voto electrónico sobre urna DRE y en colegio electoral es un sistema recomendado siempre y cuando el desarrollo del programa de puesta en marcha se haga con cuidado y con el objetivo claro de preservar los derechos democráticos básicos.

Es necesario establecer los procedimientos para la estandarización del proceso y de la máquina, a fin de verificar la seguridad, fiabilidad, eficiencia, facilidad de uso y configuración de la misma. En cuanto a las soluciones de voto electrónico sobre cualquier tipo de dispositivo conectado a una red, en general a Internet, están lejos de ser resueltos por el cúmulo de vulnerabilidades e incertidumbres que rodean a la transmisión del voto por este tipo de redes. Esto desde el punto de vista tecnológico, pero si añadimos otro tipo de problemas de corte social (coacción, compra masiva de votos, problemas jurídicos, etc.), hacen que este tipo de soluciones para el voto electoral estén lejos de ser una realidad de forma inmediata. A pesar de ello es el gran reto con el que todo el mundo sueña.

En general:

La introducción del voto electrónico tendrá que hacerse de forma gradual y razonable. Tenemos que tener en cuenta que la aparición de estas tecnologías por si solas no cambiarán las actitudes políticas de los ciudadanos. Ellas solas no podrán combatir el creciente desinterés del ciudadano por expresar su opinión en las urnas. En cambio, si se combinan las tecnologías de la información y las comunicaciones en su aplicación en las urnas con las nuevas formas de expresión y participación ciudadanas en la vida política, el resultado podría ser un incremento de la motivación del ciudadano por incorporarse de una forma activa en la vida política en todos sus niveles.

El moderno estilo de vida en el que es cotidiana la gestión de nuestra información en todos los ámbitos, incluso en los más críticos, y en la realización de nuestras compras a través de Internet, nos pueden hacer pensar que es posible su uso para expresar nuestra intención política. En realidad, el nivel de seguridad de la información en este último caso es muy superior a cualquiera de los otros usos de las TIC, ya que en el caso del voto electrónico NADIE puede llegar a conocer esta información salvo nosotros mismos y de esta forma el votante y su intención de voto se separan antes de ser procesados para no volver a ser relacionados. En cualquier otro uso, siempre hay otro extremo que puede conocer toda nuestra información con objeto de procesarla y gestionarla. Esto hace del voto electrónico un caso excepcional en el tratamiento de su seguridad por procedimientos electrónicos. Es por ello que en diversos proyectos y experiencias se cometió el error de considerar los procedimientos de seguridad en el voto como un caso más. Esto es especialmente grave cuando el voto se transmite utilizando Internet, de tal forma que es incluso hoy en día precipitado hablar de esta posibilidad como factible.

En cualquier caso es esencial que la Administración desde un primer momento dé muestras de una total transparencia en todo el procedimiento, con información clara y abierta y permitiendo la participación de todos aquellos ciudadanos interesados en aportar su opinión y conocimiento. La Administración debería consultar con los ciudadanos, la comunidad académica e investigadores y las empresas especializadas para tener en cuenta sus sugerencias y apoyos.

En el caso del voto electrónico remoto o telemático sería recomendable:

Que estos sistemas deberían utilizar técnicas que no necesitaran de aplicaciones especializadas en el cliente para garantizar la seguridad del sistema. Estas técnicas deberían de estar disponibles para todo tipo de sistemas y dispositivos. Además el sistema en su diseño no puede considerar que la red tiene suficientes mecanismos de seguridad por sí misma.

Quizá el impacto fundamental de Internet en la vida democrática se refiere a su capacidad de consolidar la esfera pública ampliando los recursos de la información, los canales de la comunicación electrónica y la capacidad de establecer una red para muchos grupos de interés organizados, movimientos sociales y organizaciones no gubernamentales. Esto incrementaría la participación ciudadana y dejaríamos el voto electrónico para ser realizado sobre urnas electrónicas en colegios electorales, con las probables ventajas de rapidez en el recuento, ahorro en las infraestructuras y en los gastos de despliegue y minimización del voto no útil (nulo), reducción de la coerción y compra de votos, etc.

Para el voto electrónico sobre urna DRE se recomienda:

El estudio de los proyectos, pruebas e implementaciones debe de estar supeditado desde el comienzo a cumplir todas y cada una de las características y requisitos detallados en el capítulo 6.1 (autentificación, anonimato, confidencialidad, integridad de los datos y del sistema, auditabilidad, eficiencia, fácil manejo y configuración, adaptabilidad a discapacitados, etc.).

Es necesario disponer de técnicas que nos permitan medir el nivel de seguridad en el sistema, para verificar que cumplen con niveles aceptables.

Deberían hacerse estudios para evaluar el nivel de precisión y seguridad de cualquier tipo de voto electrónico y determinar las características mínimas para que el sistema obtuviera la acreditación.

Deberían investigarse, con diversos tipos de pruebas, como pueden desplegarse estas tecnologías a gran escala y qué impacto tendrían sobre la sociedad. Además se deberían valorar el uso de estas tecnologías e infraestructuras para otros usos, como la participación ciudadana u otro tipo de consultas incluso de tipo privado (asociaciones, empresas, juntas de accionistas, etc.).

Los aspectos de seguridad deberían verificarse de forma continua en los siguientes aspectos: control de acceso al sistema, técnicas de codificación, seguridad física, pruebas de auditoria y almacenamiento redundante.

En los sistemas de voto electrónico deberían valorarse los siguientes aspectos: precisión, facilidad de uso, eficiencia (sobre todo velocidad en el proceso de votación), accesibilidad para discapacitados y coste.

Las fases de puesta en marcha de las pruebas deberían tener en cuenta: la preparación y diseño consensuado de la papeleta de voto, la publicidad del sistema y la formación previa del votante, la formación y entrenamiento de los responsables de las mesas, el diseño de los colegios electorales para adaptarse a este tipo de pruebas, el desarrollo de la prueba en sí y el procedimiento de escrutinio, actas y transmisión de resultados.

Para incrementar la seguridad en las DRE se recomienda: revisar todos los mecanismos de seguridad y los procedimientos asociados, impulsar el desarrollo de estándares y determinar el procedimiento para la certificación de los sistemas, valorar el uso del software con código abierto como único plenamente transparente, la utilización de arquitecturas modulares en estos sistemas que permitan separar físicamente el interfaz del votante, de la votación en sí y del proceso de escrutinio, desarrollar los protocolos de seguridad para permitir al votante, antes y después del escrutinio, verificar que su voto no ha sido manipulado u omitido.

Trabajos futuros.

Lecciones aprendidas y primeros pasos en el camino correcto: la necesidad de la auditoría extremo a extremo en los procesos de VE. Esta solución parece ser a día de hoy, como la más viable, elaborada y mejor diseñada. En la práctica pocas veces ha sido puesta a prueba [48] e incluso, según algunos autores, podrían aparecer problemas con la interpretación del secreto del voto [51] [52].

Por todo ello el debate sigue abierto y es necesario mantenerse informado. Esto no es óbice para que el VE pueda seguir siendo utilizado en lugares y circunstancias en las que no existe otra solución adecuada, ya sea por dificultades orográficas, de movilidad, de circunstancias personales o cualquiera otra que nos impida o dificulte expresar nuestro voto u opinión, base de la democracia que no debería conculcarse por ninguna razón.

# 11. Referencias y documentación

|  |  |
| --- | --- |
| [1] | Council of Europe Committee of Ministers, *Legal, operational and technical standards for e-voting, rec(2004),* Bruselas: Council of Europe Committee of Ministers, 2004. |
| [2] | J. Carracedo Gallardo y E. Pérez Belleboni, «Voto electrónico, voto telématico y voto por Internet: requisitos socialmente demandados y técnicamente viables.,» de *Democracia digital, participación y voto electrónico*, Valencia, Fundación Centro de Estudios Políticos y Sociales, 2010, p. 200. |
| [3] | E. Belleboni, Aplicación de documentos de identificación electrónica a un esquema de voto telemático a escala paneuropea, seguro, auditable y verificable. Tesis doctoral, Madrid: Universidad Politécnica, 2013. |
| [4] | Gobierno de España, Ministerio del Interior. Dirección general de política interior., 2010. [En línea]. Available: http://www.infoelectoral.mir.es/EnlacesInteres/enlaces\_mae.html. [Último acceso: 2013 5 26]. |
| [5] | H. K. Prasad, J. A. Halderman, R. Gonggrijp y et al., «Security Analysis of India’s Electronic Voting Machines,» de *17th ACM Conference on Computer and Communications Security (CCS ’10)*, Chicago, 2010. |
| [6] | A. B. Filho y M. A. Cortiz, Fraudes e Defesas no voto electronico, Sao Paulo, Brasil: All Print , 2006. |
| [7] | M. Torre y L. Panizo, «Technological Solutions for Electronic Voting and Guarantees of the Integrity of the Electoral Process. A Case Study,» 10 10 2012. [En línea]. Available: http://hdl.handle.net/10612/2845 [Último acceso: 09 12 2013]. |
| [8] | J. Carracedo Gallardo, Seguridad en redes telemáticas, Madrid: McGRAW-HILL, 2004. |
| [9] | R. C. Hite, «Electronic voting offers, opportunities and presents challenges.,» U.S. Govermment Accountability Office, Washington, 2004. |
| [10] | C. McCormack, «Re-counting the vote: What does it cost? Pew Charitable Trusts,» 01 10 2010 [En línea]. Available: http://www.pewstates.org/uploadedFiles/PCS\_Assets/2010/Pew\_Cost\_of\_Recounts\_report.pdf . [Último acceso: 13 07 2013]. |
| [11] | Saveour Votes, «Analysis of the Cost of Procuring and Implementingan Optical Scan Voting System in Maryland.» 04 03 2011. [En línea]. Available: http://www.saveourvotes.org/reports/2010/2010-3-04sov-costanalysis.pdf. [Último acceso: 13 07 2013]. |
| [12] | I. D. Fernández, «El voto electrónico.» *Revista del Ilustre Colegio de Abogados de Madrid,* 2003. |
| [13] | M. Cantijoch , «El voto electrónico ¿ un temor justificado ?» *TEXTOS de la Cibersociedad ,* nº 7, 2005. |
| [14] | C. Cox y A. Rubin, «Is the U.S. ready for electronic voting?» *New York Times Upfront,* 20 09 2004. |
| [15] | B. Adida, Advances in cryptographic voting systems, Massachusetts: Thesis (Ph. D.)--Massachusetts Institute of Technology, Dept. of Electrical Engineering and Computer Science., 2006. |
| [16] | R. Mercuri, «www.notablesoftware.com/» 2001. [En línea]. Available: www.notablesoftware.com/RMstatement.html. [Último acceso: 27 08 2013]. |
| [17] | R. Mercuri, Electronic Vote Tabulation: Checks and Balances., Philadelphia: PhD thesis, University of Pennsylvannia, 2001. |
| [18] | T. Kohno, A. Stubblefield, A. A. Rubin y D. S. Wallach, «Analysis of an electronic voting system» *Security and Privacy,* pp. 27 - 40, 2004. |
| [19] | C. Armen y R. Morelli, «E-voting and computer science» de *ACM ITiCSE´05*, Monte de Caparica, Portugal,, 2005. |
| [20] | A. Di Franco, A. Petro, E. Shear y V. Valdiimirov, «Small vote manipulations can swing elections» *Communications of the ACM,* vol. 47, nº 10, pp. 43-45, 2004. |
| [21] | G. Schryen , «Security aspects of Internet Voting» de *Proceedings of the 37th Hawai International Conference on Systems Sciences*, Island of Hawaii , 2004. |
| [22] | G. Schryen, «E-Democracy: Internet Voting» de *Proceedings of the IADIS International Conference 2003*, Algarve, Portugal, 2003. |
| [23] | D. Jefferson, A. D. Rubin y et al, «Analyzing Internet Voting Security» *Communications of the ACM,* vol. 47, nº 10, pp. 59-64, 2004. |
| [24] | C. K. Wu y R. Sankaranarayana, «Internet voting: Concerns and solutions.» de *Proceedings of the first International Symposium on Cyberworlds (CW´02)*, Tokyo, JAPAN, 2002. |
| [25] | R. Anane, R. Freeland y G. Theodoropoulos, «e-voting requirements and implementation» de *9th IEEE International Conference on E-Commerce Technology* , Tokyo, Japan, 2007. |
| [26] | K. Daimi, K. Snyder y R. James, «Requirements Engineering for E-Voting Systems.» *Software Engineering Research and Practice,* pp. 259-265, 2006. |
| [27] | S. Ikonomopoulos, C. Lambrinoudakis, D. Gritzalis, S. Kokolakis y K. Vassiliou, «Functional requirements for a secure electronic voting system.» de *Security in the Information Society: Visions and Perspectives, IFIP TC11 17th International Conference on Information Security (SEC2002)*, Cairo,Egypt, 2002. . |
| [28] | G. Z. Qadah y R. Taha, «Electronic voting systems: Requirements, design, and implementation.» *Computer Standards & Interfaces,* pp. 376-386, 2007. |
| [29] | M. Volkamer y M. Mcgaley, «Requirements and evaluation procedures for evoting» de *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference* , Viena, Austria, 2007. |
| [30] | K. Weldemariam, A. Mattioli y A. Villafiorita, «Managing Requirements for E-Voting Systems: Issues and Approaches.» de *Requirements Engineering for e-Voting Systems (RE-VOTE), 2009 First International Workshop* , Atlanta, Georgia, 2009. |
| [31] | R. Mercuri, «Voting-machine risks» *Commun. ACM,* vol. 11, nº 35, p. 138, 1992. |
| [32] | D. W. Jones y B. Simons, Broken ballots. Will your vote count?, Stanford, California: CSLI Publications, 2012. |
| [33] | D. Aranha, M. M. Karam, A. Miranda y F. Scarel, «Software Vulnerabilities in the Brazilian Voting Machine» de *Electronic Voting Tech. Workshop*, Bellevue, Washington, 2012. |
| [34] | S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati y S. K. Sakhamuri, « Security analysis of India's electronic voting machines» 2010. [En línea]. Available: http://indiaevm.org/evm\_tr2010.pdf . [Último acceso: 2013 06 06]. |
| [35] | R. L. Rivest, «Some thoughts on electronic voting» 26 5 2004. [En línea]. Available: http://people.csail.mit.edu/rivest/pubs.html#Riv04a. [Último acceso: 25 5 2013]. |
| [36] | B. Schneier, «Opendemocracy» 09 11 2004. [En línea]. Available: http://www.schneier.com/essay-068.html. [Último acceso: 16 07 2013]. |
| [37] | A. Gumbel, Steal This Vote: Dirty Elections and the Rotten History of Democracy in America, Nations Books, 2005. |
| [38] | H. Alaiz, L. Panizo, R. A. Fernández y J. Alfonso, «Technical Audit of an Electronic Polling Station: A Case Study» *International Journal of E-Services and Mobile Applications (IJESMA),* vol. 3, nº 3, p. 15, 2011. |
| [39] | J. Barrat, «http://www.idea.int/» Idea, [En línea]. Available: http://www.idea.int/democracydialog/upload/Observing-e-enabled-elections-how-to-implement-regional-electoral-standards.pdf [Último acceso: 03 12 2013]. |
| [40] | D. Chaum y et al, «Scantegrity: end-to-end voter-verifiable optical-scan voting» *IEEE Security & Privacy,* vol. May/Jun , pp. 40-46, 2008. |
| [41] | D. Chaum, P. Y. A. Ryan y S. Schneider, «A practical voter-verifiable election scheme» *Proceedings of the 10th European conference on Research in Computer Security,* vol. 1, nº 1, pp. 118-139, 2005. |
| [42] | P. Y. A. Ryan, D. Bismark, J. Heather y S. Schneider, «Prêt à Voter: a Voter-Verifiable Voting System» *Information Forensics and Security,* vol. 4, nº 4, pp. 662 - 673, 2009. |
| [43] | D. Bismark, J. Heather, R. M. A. Peel, S. Schneider y P. Y. Ryan, «Experiences Gained from the first Prêt à Voter Implementation» *Requirements Engineering for e-Voting Systems (RE-VOTE),* vol. 1, nº 1, pp. 19-28, 2009. |
| [44] | R. L. Rivest, «The ThreeBallot Voting System» 1 10 2006. [En línea]. Available: http://theory.csail.mit.edu/~rivest/Rivest-TheThreeBallotVotingSystem.pdf. [Último acceso: 26 11 2013]. |
| [45] | B. Adida y R. L. Rivest, «Scratch & Vote. Self-Contained Paper-Based Cryptographic Voting» *WPES’06,* vol. October, pp. 29-35, 2006. |
| [46] | A. Kiayias, M. Korman y D. Walluck, «An Internet Voting System Supporting User Privacy» *Computer Security Applications Conference,* vol. 22, nº 1, pp. 165 - 174, 2006. |
| [47] | B. Adida, «Helios: web-based open-audit voting» *Proceedings of the 17th conference on Security symposium,* vol. 1, nº 8, pp. 335-348, 2008. |
| [48] | B. Adida, O. De Marneffe, O. Pereira y J.-J. Quisquater, «Electing a university president using open-audit voting: analysis of real-world use of Helios» *EVT/WOTE'09 Proceedings of the 2009 conference on Electronic voting technology/workshop on trustworthy elections,* vol. 1, nº 1, pp. 10-10, 2009. |
| [49] | S. Chasteen, «Electronic voting unreliable without receipt, expert says» *Stanford Report,* pp. http://news.stanford.edu/news/2004/february18/aaas-dillsr-218.html, 18 02 2004. |
| [50] | Helios Voting, «heliosvoting.org» Helios Voting, [En línea]. Available: https://vote.heliosvoting.org/. [Último acceso: 03 12 2013]. |
| [51] | D. W. Jones, «http://homepage.cs.uiowa.edu/~jones/voting» 2009. [En línea]. Available: http://homepage.cs.uiowa.edu/~jones/voting/E2E2009.pdf [Último acceso: 04 12 2013]. |
| [52] | S. Popoveniuc, J. Kelsey, A. Regenscheid y P. Vora, «https://www.usenix.org/legacy/event/evtwote10/tech/full\_papers» 04 12 2010. [En línea]. Available: https://www.usenix.org/legacy/event/evtwote10/tech/full\_papers/Popoveniuc.pdf. [Último acceso: 2013]. |
| [53] | Parlamento Escocés, «http://www.scottish.parliament.uk» [En línea]. Available: http://www.scottish.parliament.uk/gettinginvolved/petitions/ [Último acceso: 03 12 2013]. |
| [54] | Florida Department of State, «Official Results November 7, 2000» 07 11 2000. [En línea]. Available: http://election.dos.state.fl.us/elections/resultsarchive/SummaryRpt.asp?ElectionDate=11/7/2000&Race=PRE&DATAMODE [Último acceso: 13 08 17]. |
| [55] | Verified Voting, «https://www.verifiedvoting.org» verifiedvoting.org, [En línea]. Available: https://www.verifiedvoting.org/verifier/ [Último acceso: 03 12 2013]. |
| [56] | A. D. Rubin, «http: //avirubin.com/» October 2004. [En línea]. Available: http://www.democraticunderground.com/discuss/duboard.php?az=view\_all&address=132x2913485. [Último acceso: 20 5 2013]. |
| [57] | Johns Hopkins University, «http://isi.jhu.edu/» Johns Hopkins University, [En línea]. Available: http://isi.jhu.edu/ [Último acceso: 03 12 2013]. |
| [58] | National Science Foundation , «http://www.nsf.gov/» NSF, [En línea]. Available: http://www.nsf.gov/ [Último acceso: 03 12 2013]. |
| [59] | Department of Justice, «http://www.justice.gov/» justice.gov, [En línea]. Available: http://www.justice.gov/crt/about/vot/hava/hava.php. |
| [60] | Ciencias y cosas, «http://cienciasycosas.wordpress.com» wordpress.com, [En línea]. Available: http://cienciasycosas.wordpress.com/2013/01/06/el-fraude-del-voto-electronico-en-las-elecciones-de-rio-do-janeiro/ [Último acceso: 03 12 2013]. |
| [61] | Concil of Europe, «http://www.coe.int» 25 03 2004. [En línea]. Available: http://www.coe.int/t/dgap/democracy/activities/GGIS/E-voting/Work\_of\_e-voting\_committee/02\_Agendas\_and\_Reports /49IP1(2004)30\_Report\_Las\_Palmas\_en.asp [Último acceso: 28 11 2013]. |
| [62] | COUNCIL OF EUROPE. COMMITTEE OF MINISTERS, «https://wcd.coe.int» 30 09 2004. [En línea]. Available: https://wcd.coe.int/ViewDoc.jsp?id=778189 [Último acceso: 28 11 2013]. |
| [63] | Auntamiento de Jun, «http://www.ayuntamientojun.org» ayuntamientojun.org, [En línea]. Available: http://www.ayuntamientojun.org/cedj [Último acceso: 03 12 2013]. |
| [64] | Observatorio del voto electrónico, «http://www.votobit.org,» votobit.org [En línea]. Available: http://www.votobit.org/misiones/pruebas/informes.html [Último acceso: 03 12 2013]. |
| [65] | Observatorio del voto electrónico, «http://www.votobit.org/» votobit.org, [En línea]. Available: http://www.votobit.org/archivos/participaespaniol.pdf [Último acceso: 03 12 2013]. |
| [66] | La Vanguardia, «http://www.lavanguardia.com» lavanguardia.com, [En línea]. Available: http://www.lavanguardia.com/vida/20100516/53928946995/el-fracaso-de-la-consulta-de-la-diagonal-se-lleva-por-delante-al-primer-teniente-de-alcalde.html [Último acceso: 03 12 2013]. |
| [67] | El Confidencial, «http://www.elconfidencial.com» elconfidencial.com, [En línea]. Available: http://www.elconfidencial.com/espana/2011/policia-ministerio-del-interior-telefonica-20110705-80985.html [Último acceso: 03 12 2013]. |
| [68] | Gobierno de Estonia, «http://www.vvk.ee» vvk.ee, [En línea]. Available: http://www.vvk.ee/voting-methods-in-estonia/engindex [Último acceso: 04 12 2013]. |
| [69] | Serve security report, «http://www.servesecurityreport.org/» .servesecurityreport.org, [En línea]. Available: http://www.servesecurityreport.org/ [Último acceso: 03 12 2013]. |
| [70] | Observatorio del voto electrónico, «http://www.votobit.org/» votobit.org, [En línea]. Available: http://www.votobit.org/misiones/pruebas/2m6.html [Último acceso: 03 12 2013]. |
| [71] | Scytl, «http://www.scytl.com» scytl.com, [En línea]. Available: http://www.scytl.com [Último acceso: 03 12 2013]. |
| [72] | Indra, «indracompany.com» Indra, [En línea]. Available: http://www.indracompany.com/soluciones-y-servicios/solucion/Procesos%20Electorales [Último acceso: 04 12 2013]. |
| [73] | Compañia Smartmatic, «http://www.smartmatic.com/espanol/principal/» Smartmatic, [En línea]. Available: http://www.smartmatic.com/espanol/principal/ [Último acceso: 04 12 2013]. |
| [74] | Diebold, «www.diebold.com» diebold.com, [En línea]. Available: www.diebold.com [Último acceso: 03 12 2013]. |

Libros:

Rubin, Aviel D. *Brave new ballot.* Morgan Road Books, New York, 2006. 978-0-7679-2210-4

Alvarez, R. Michael *Point, Click and Vote. The future of Internet voting.* Brookings Institution Press, Washington, D.C., 2004. 0-8157-0368-6

Jones, Douglas; Simons, Barbara *Broken ballots: will your vote count in the electronic age?* CSLI Publications, Stanford, CA, 2012. 978-1-57586-637-6

Martínez Dalmau, Rubén *Voto electrónico, democracia y participación.* Valdell hermanos, Caracas, 2006. 980-212-428-1

Páginas web:

Plataforma Voto-e. <http://www.votoe.es/>

Observatorio del Voto-E en Latinoamerica. <http://www.voto-electronico.org/>

Observatorio Voto Electrónico (España) <http://www.votobit.org/>

Competence Center for Electronic Voting and Participation <http://www.e-voting.cc/en/>