VOTO ELECTRÓNICO

UN APORTE TÉCNICO-CIENTÍFICO A LA REFORMA ELECTORAL

ALEJANDRO HÉCTOR MOLINA
MABEL NOEMI BOTTONI
CLAUDIA LILIAN GARCIA

Prólogo

CLAUDIO C. BARGACH

RED ENCUENTRO CIUDADANO PARA LA CALIDAD DEMOCRÁTICA rec

Ser Fiscal

Friedrich Naumann STIFTUNG FÜR DIE FREIHEIT

ALEJANDRO HÉCTOR MOLINA, MABEL NOEMI BOTTONI Y CLAUDIA LILIAN GARCIA
VOTO ELECTRÓNICO UN APORTE TÉCNICO-CIENTÍFICO A LA REFORMA ELECTORAL
©REC Red Encuentro Ciudadano
Apoyo Friedrich Naumann
Editado por REC
ISBN 978 987 3677 56 4

Grupo Unión
union@lugardelibros.com
lugardelibros.com
@unioneditorial
Coordinación editorial Rodolfo Distel (@rdistel)
Composición por #MCHFS

Impreso en la República Argentina por LA IMPRENTA YA SRL
Reservados todos los derechos. El contenido de esta obra está protegido por las leyes, que establecen penas de prisión y multas, además de las correspondientes indemnizaciones por daños y perjuicios, para quienes reprodujeran total o parcialmente el contenido de este libro por cualquier procedimiento electrónico o mecánico, incluso fotocopia, grabación magnética, óptica o informática, o cualquier sistema de almacenamiento de información o sistema de recuperación, sin permiso escrito del editor.

ÍNDICE

VOTO ELECTRÓNICO: LA VISIÓN DE LA RED SER FISCAL
por Claudio C. Bargach 7

I - INTRODUCCIÓN

II - QUÉ ES EL VOTO ELECTRÓNICO

II.1.- Dimensiones del voto electrónico 18
II.2.- Desarrollo e implementación del Voto Electrónico 19

III -EL VOTO ELECTRÓNICO EN EL MUNDO

III.1.- Sistemas de urna electrónica 27
III.1.1.- Alemania 27
III.1.2.- Australia 29
III.1.3.- Bélgica 30
III.1.4.- Emiratos Árabes Unidos 31
III.1.5.- España 31
III.1.5.- Finlandia 35
III.1.7.- Francia 36
III.1.8.- Holanda 37
III.1.9.- India 38
III.1.10.- Irlanda 42
III.1.11.- Japón 42
III.1.12.- Kazajistán 45
III.1.13.- Noruega 45
III.1.14.- Rusia 46
III.2.- Sistemas con uso de la tecnologia celular 47
III.2.1.- Canadá 47
III.2.2.- Corea del Sur 50
III.2.3.- Estonia 52
III.2.4.- Reino Unido 53

III.2.5.- Suiza 55
III.3.- Sistemas Mixtos 57
III.3.1- E.E.U.U. 57
III.3.2.- Filipinas 59
III.4.- Conclusiones sobre el uso del voto electroniónico en distitnos países 60

IV - EXPERIENCIAS EN AMÉRICA LATINA

IV.1.- Detalle de las Experiencias en cada país 65
IV.1.1.- Brasil 65
IV.1.2.- Colombia 69
IV.1.3.- Costa Rica 74
IV.1.4.- Ecuador 75
IV.1.5.- Guatemala 75
IV.1.6.- México 75
IV.1.7.- Panamá 76
IV.1.8.- Paraguay 76
IV.1.9.- Perú 79
IV.1.10.- Venezuela 83
IV.2.- Conclusiones sobre las experiencias de Latinoamérica 85

V - EXPERIENCIAS EN ARGENTINA

V.1.- Provincia de Buenos Aires 88
V.2.- Ciudad de Posadas. Misiones 89
V.3.- Otras experiencias 90

VI - PROPUESTA DE USO DE LA TECNOLOGÍA EN UNA ELECCIÓN

VI.1.- Etapa pre electoral 100
VI.2.- Etapa Electoral 105
VI.3.- Etapa Post electoral 107
VI.1.- Escrutinio Definitivo 108

VII - PROPUESTA DE TRABAJO PARA EL DESARROLLO DE UN SISTEMA ELECTORAL

VII.1.- Características 111
VII.2.- Participantes 113
VII.3.- Organización de los Participantes 116

VIII - CONCLUSIONES Y RECOMENDACIONES

VIII. 1.- Conclusiones 119

ANEXO A - SOFTWARE LIBRE: IMPRESCINDIBLE PARA EL SISTEMA DE VOTO ELECTRÓNICO

A.1.- Cómo es en gerneal la gestión de un proyecto de Software Libre
A.1.1.- Qué herramientas se usan en la gestión 134
A.1.2.- Qué sucede en el desarrollo de Software Libre 135
A.2.- Formas de gestión del desarrollo de software
A.2.1.- Modelo Cascada 138
A.2.2.- Modelo Espiral 139
A.2.3.- Modelo Iterativo o Incremental 139
A.2.4.- Descripción de las actividades básicas del desarrollo

A.2.4.1.- Análisis de requisitos 141
A.2.4.2.-Estimación de costes 142
A.2.4.3.-Diseño 143
A.2.4.4.-Documentación 144
A.2.4.5.-Pruebas y calidad 145
A.2.4.6.-Seguridad 147

ANEXO B - EMPRESAS, PRODUCTOS Y ESTÁNDARES
B.1.- Estándares 151

ANEXO C - SISTEMAS DE VOTACIÓN VERIFICABLES DE EXTREMO A EXTREMO (E2E)
C.1.- Punchscan 159
C.2.- Scantegrity 164
C.3.- Threeballot 171
C.4.- Scratch&Vote 176
C.5.- Prêt à voter 181
C.6.- Bingo Voting 185

BIBLIOGRAFÍA 196

LOS AUTORES 202

EL EQUIPO DE SER FISCAL 203

VOTO ELECTRÓNICO: LA VISIÓN DE LA RED SER FISCAL

La RED SER FISCAL es una organización ciudadana, voluntaria, no partidaria, que ha tomado como uno de sus desafíos contribuir de distintas maneras a la Transparencia Electoral por una mejor República.

Cualquier lector, mínimamente informado, podrá constatar, que a 100 años de la elección del primer presidente constitucional a través de la Ley 8871 llamada Ley Sáenz Peña de voto universal masculino secreto y obligatorio, hay desafíos que por la transparencia electoral aún debemos asumir y solucionar.

Las dificultades del derecho constitucional de elegir y ser elegido en el acto eleccionario muestran algunas cuestiones de pendiente solución. Existe un amplio consenso de partidos políticos, organizaciones no gubernamentales especializadas en la temática, constitucionalistas, académicos y expertos, que consideran al año 2016 por su connotación no electoral, el momento oportuno para impulsar una reforma política que nos encamine a

mejorar notablemente el objeto constitucional de nuestros desvelos.

Sin dudas que la Boleta Única Electrónica (BUE) tiene una marcada simpatía en los distritos donde se ha utilizado, como en diversos ámbitos políticos donde se la ha impulsado .Si bien, la Boleta Única en papel (BU) tiene también sus defensores, esta disputa, que la saldará el Congreso Nacional, genera la necesidad de este material científico y de política electoral que hoy llega a vuestra consideración. Desde la perspectiva de los autores se realiza un estudio y análisis sobre el voto electrónico y diversas alternativas en torno al mismo.

Consideramos esencial, alejar los temores o sospechas sobre las cuestiones tecnológicas, y para ello nada mejor que generar procesos abiertos, participativos, con eficaces controles y particularmente, con la propiedad intelectual del software en poder del Estado, facilitador de un aporte de la comunidad interesada en la temática y en su control.

El sistema de votación es un aspecto importante, pero uno más de una profunda reforma electoral. Hay un solo sistema electoral que funciona, el realizado como política de estado con el más amplio consenso.

Sirva este aporte científico, fruto de la demanda y experiencia ciudadana de la RED SER FISCAL, con el trabajo profesional de expertos argentinos nucleados en el “Grupo de Estudios sobre Tecnologías Electorales”, para contribuir a generar el único sistema electoral que funciona, “el de la confianza”.

Llega a vuestras manos este trabajo, producto del esfuerzo voluntario de profesionales especializados y el apoyo decidido de la FUNDACIÓN F. NAUMANN PARA LA LIBERTAD , quién reiteradamente nos asiste en pos de contribuir a una mejor REPÚBLICA y la TRANSPARENCIA ELECTORAL.

Claudio C. Bargach
COORDINADOR NACIONAL
RED SER FISCAL

I
INTRODUCCIÓN

Existen distintas definiciones del llamado comúnmente "voto electrónico". Siguiendo a Fadiño Casas (FADIÑO CASAS, 2012), se considera voto electrónico a la incorporación de recursos informáticos en cualquier parte del proceso electoral, la logística electoral, la emisión del voto, el escrutinio y la transmisión de los resultados.

Las Tecnologías de la Información y la Comunicación han permitido, que los organismos públicos implementen soluciones tecnológicas en sus procedimientos administrativos y logísticos, en su labor cotidiana. Así, la mayoría de los organismos electorales han automatizado sus padrones electorales, el acto de votación y el escrutinio, con diferentes tecnologías, como la biométrica, pantallas sensibles al tacto y software incorporados de máquinas de votación, que realizan el conteo.

Todo esto ha llevado a incorporar en las discusiones de los procesos electorales términos, como "voto electrónico", " e-democracia", "voto telemático", "tecnopolítica", "voto informático", "tecnodemocracia", "voto informatizado", "democracia digital", "ciberdemocracia", "teledemocracia" o "democracia electrónica"

A pesar de las numerosas definiciones que se han dado, todavía tiene sentido preguntarse ¿Qué es el voto electrónico?, ya que este cambia constantemente, y se adapta con distintas características al desarrollo de las innovaciones que surgen de la informática y las comu-

nicaciones. Por ello, el análisis político de los sistemas electorales trata de incorporarlo mas como una característica de la sociedad del siglo XXI, que como un hecho concreto. El surgimiento de la "Sociedad de la Información" ha generado un gran impacto en la aplicación de las nuevas tecnologías al contexto político-electoral, convirtiéndose en una tendencia, que influye en el derecho electoral y por ende en los procesos de votación.

Aunque, para hablar de voto o democracia electrónica, muchos autores coinciden en, que esta construcción conceptual, resulta insuficiente ante el entorno tecnológico en el que nos encontramos inmersos; algunos autores se cuestionan si no es posible que la democracia electrónica encubra una dictadura de expertos, o si la utilización de la tecnología modificará el proceso democrático mejorando la comunicación política y el conocimiento de las aspiraciones de los ciudadanos.

Si bien, existen antecedentes en países desarrollados, en la década del noventa se realizaron las primeras experiencias de voto electrónico, utilizando distintas modalidades. Si bien el avance producido fue complejo, actualmente hay países que han automatizado el voto electrónico en la totalidad de sus mesas electorales.

Los sistemas de tecnificación del voto electrónico, para muchos países, suelen venir de la mano de una mayor transparencia en el proceso electoral, la eliminación del clientelismo político, la rapidez e infalibilidad del conteo, el menor costo de cada elección, y la mayor participación ciudadana.

A pesar que la aplicación de las nuevas tecnologías conlleva una serie de riesgos, todo avance tecnológico es susceptible de modificaciones, por lo que se deben adoptar las medidas legislativas que regulen el uso y la manipulación de las herramientas electrónicas, que darán paso al uso del voto electrónico por parte de los ciudadanos.

La introducción de nuevas tecnologías en los procesos electorales plantea la necesidad de introducir nuevos mecanismos electorales y modificar instituciones jurídico-electorales, con el fin de garantizar la transparencia y el adecuado manejo de la información electoral. El presente trabajo trata de exponer algunas experiencias mundiales, latinoamericanas y algunos antecedentes de Argentina. También analiza la incorporación de la tecnología al proceso electoral y se plantea el uso de software libre como alternativa tecnológica que garantizaría la transparencia del proceso del voto electrónico.

II
QUE ES EL VOTO ELECTRÓNICO

En sentido amplio, se entiende por voto electrónico aquel en el que se introducen las nuevas tecnologías existentes, principalmente las tecnologías de la Información y las Comunicaciones, en alguna, o todas las fases del proceso electoral (emisión de votos, escrutinio, transmisión de datos, padrón electoral, etc.).

En sentido estricto, se refiere a la utilización de medios electrónicos para la emisión de votos y su recuento.

Para una clasificación inicial se pueden considerar los sistemas de emisión de voto remota y los sistemas de emisión de voto presencial. En el primer sistema se trata de la utilización de internet para ejercer el acto de votar, ya sea a través de una computadora, un dispositivo celular u otro que posea los requerimientos necesarios para acceder a una red, permitiendo el ejercicio del sufragio a distancia.

En el caso del sistema de emisión de voto presencial, el elector debe concurrir al lugar de votación para la emisión del voto. La única diferencia con el sistema tradicional de votación, es la herramienta utilizada para emitir el voto. Este último sistema es el que se encuentra vigente en la República Argentina. En la actualidad el Código Electoral Nacional, las leyes electorales provinciales y las leyes electorales de la CABA sólo admiten el sistema de emisión de voto presencial.

El sistema de emisión de voto remota es complejo y actualmente muy pocos países se encuentran con posibilidades reales de implementarlo de forma masiva. Muchos países aún muestran suspicacias respecto a permitir que sus ciudadanos emitan sus votos mediante Internet y la telefonía celular, pues se duda de los sistemas de seguridad de los servidores, que potencialmente pueden alterar los votos y, por consiguiente, la voluntad ciudadana. Este tipo de tecnología sólo es viable en sociedades con un alto grado de alfabetización tecnológica, y que cuentan con un elevado nivel de desarrollo de la infraestructura necesaria para darle cobertura de red y satelital a casi el 100% de su población, algo que muy pocos países en el mundo pueden hacer en la actualidad. Sin embargo, a medida que los gobiernos vayan impulsando el aumento de los servicios de Internet y la telefonía celular, y su presencia en la vida cotidiana penetre aún más, no se duda, que estas tecnologías también jugarán un importante papel en las elecciones futuras de muchos países.

En el sistema de emisión de voto presencial, existen dos grandes grupos: los Sistemas de Lectura Óptica de Votos (LOV) y los Sistemas de Registro Electrónico Directo (RED). Los Sistemas de Lectura Óptica de Votos (LOV), son aquellos donde el voto se realiza mediante la utilización de una boleta electoral, que será posteriormente leída por la máquina de votación. La boleta se deposita manualmente en una urna electoral y se conserva la boleta como comprobante tangible del voto. Se trata de un sistema de automatización de recuento de votos mediante la utilización de un scanner óptico que reconoce los

datos insertos en la boleta en la oportunidad de efectuar el escrutinio provisorio.

En el caso de la Boleta Única Electrónica, utilizada en Salta y en la Ciudad Autónoma de Buenos Aires, se conserva la boleta como comprobante papel del voto, permitiendo un control manual de los votos además del electrónico – al quedar almacenado en un chip de tipo RFID (Radio Frequency IDentification) contenido en la boleta-.

Los Sistemas de Registro Electrónico Directo (RED), son aquellos donde el voto se emite electrónicamente. Se registra directamente el voto mediante su lectura en un dispositivo informático, convirtiendo en innecesario el uso de la boleta papel. Muchos advierten las ventajas de estos sistemas, habida cuenta que en el escrutinio provisorio no habría posibilidad de manipulación de los datos, reduciéndose, de manera considerable, el error del conteo con la automatización en la impresión del acta de escrutinio.

Un esquema de los sistemas descriptos se puede apreciar en la siguiente tabla:

Tabla I. Sistemas de Voto Electrónico

Sistemas de Voto Electrónico	Sistemas de Emisión Remota	Boleta WEB Electrónica – BWE
	Sistemas Presenciales	Sistemas de Lectura Óptica de Votos - LOV
		Sistemas de Registro Electrónico Directo - RED

En la actualidad se ha avanzado hacia los llamados sistemas de votación verificables de extremo a extremo (End-to-End auditable voting systems o sistemas E2E) que

proponen una solución frente a la necesidad de mantener el anonimato y asegurar la fiabilidad de los protocolos de votación, y se caracterizan por su integridad y seguridad ante los intentos de adulterar el voto, empleando métodos de cifrado complejos para elaborar comprobantes que permitan a los votantes verificar que sus votos han sido contabilizados correctamente sin poner en peligro el secreto del voto (FINK, 2010). Un detalle de estos sistemas se agrega como anexo al presente trabajo.

II.1.- Dimensiones del Voto Electrónico

Para abordar la cuestión en torno a la incorporación del voto electrónico, se deben tener en cuenta fundamentalmente el contexto político, social, las instituciones de la administración electoral y, por supuesto, las nuevas tecnologías.

En una sociedad con mayor desconfianza hacia la política, seguramente habrá más resistencia al cambio. En un contexto socio-político en el que se percibe un gran descreimiento en las instituciones del Estado y en los procedimientos electorales a su cargo, resulta necesario buscar el consenso de todos los actores (ciudadanos, partidos políticos, gobiernos en turno, organizaciones de la sociedad civil, universidades), para generar una verdadera transformación. En un contexto de profunda crisis de insatisfacción con el funcionamiento de la democracia, en el que se cuestiona la eficacia de sus instituciones para resolver los problemas que afligen a la sociedad, se requiere un Estado activo y con instituciones honestas y transparentes en la gestión pública. Asimismo, es impor-

tante que la ciudadanía reconozca las causas del problema y decida que necesita cambiar.

Se debe tener en claro que las prioridades tecnológicas no se encuentran por encima de los factores políticos y sociales. Considerar, que la implementación del voto electrónico, significa un avance hacia las nuevas tecnologías y que, sólo por ello, será aceptado en la comunidad, no resulta una mirada correcta.

La tecnología avanza muy rápido y las leyes que deben instrumentar su incorporación requieren un procedimiento más extenso y lento. Por ello, es fundamental involucrar a los actores políticos y sociales, que intervienen en el proceso, para cambiar el marco legal de las elecciones y, así, no retrasar su implementación.

II.2.- Desarrollo e Implementación del Voto Electrónico

La implementación del sistema de voto electrónico, debe llevarse adelante dentro de un complejo entramado social, político, legal y electoral. Para ello, el proceso de desarrollo e implementación del sistema de voto electrónico, debe ser coordinado con todos los actores políticos y sociales estableciéndose objetivos mensurables y plazos. Conjuntamente, se deben generar extensas e intensas campañas de concientización social y capacitación de la ciudadanía.

Para generar confianza social hacia el sistema que se desea implantar, se debe generar interacción con diversos sectores sociales tales como universidades, organizaciones de la sociedad civil, proveedores e industrias nacionales. Ello así, toda vez que la investigación en las

universidades cuenta en general con aceptación social y la cooperación con organizaciones de la sociedad civil aumenta el compromiso sobre el proceso de desarrollo e implementación.

El desarrollo e implementación del voto electrónico, debe darse, dentro de los siguientes principios básicos de la administración electoral:

- Independencia en la gestión;
- Inexistencia de influencia negativa de los partidos políticos;
- Respeto a la ley;
- Profesionalismo, expertos/técnicos en seguridad informática;
- Procesos y actores tecnológicos subordinados a instrucciones político-institucionales;
- Garantizar transparencia del Sistema de Voto Electrónico.

La implementación del sistema de voto electrónico, debe asegurar la observancia de los principios fundamentales democráticos del voto (universalidad, secreto, integridad y auditabilidad). Se debe salvaguardar la seguridad del voto. Por ello, es importante que la reforma legislativa establezca los marcos reguladores sobre los mecanismos de control y seguimiento del sistema. Algunas medidas, necesarias, para la adopción del Sistema de Voto Electrónico, en palabras de María Inés Tula (TULA, 2005), serían:

- Un Estado garante, que asuma un papel fundamental en la regulación normativa de los procesos de modernización tecnológica.

- La modernización de las primeras fases del proceso electoral.
- Gradualidad en la implementación del sistema.
- Asegurar una infraestructura de telecomunicaciones mínimas.
- Realizar campañas de difusión pública y de concientización ciudadana.
- Garantizar la transparencia del sistema, mediante el acceso al código fuente y a los registros de funcionamiento.
- Garantizar la auditabilidad de todo el proceso electoral.
- Implementar la incorporación de un comprobante físico de voto.
- Actualizar las normas existentes en materia de seguridad (delitos informáticos).

Estas medidas se deben complementar, con otras que garanticen la transparencia y la seguridad en los siguientes procesos:

Control y supervisión durante el proceso de diseño y ejecución del hardware y del software.
Garantizar que el mantenimiento impida conexiones indeseadas de los equipos utilizados.
Es aconsejable utilizar hardware de dominio público.
Se deben encriptar los datos que se transmitan con un protocolo de doble verificación, para que la información no pueda ser vulnerada y se mantenga el secreto del voto.
Garantizar el acceso al código fuente.
La incorporación del comprobante físico de voto.

El Control en el recuento de votos mediante técnicas de muestreo.

Debe destacarse, que dos aspectos resultan esenciales, para garantizar la transparencia de los comicios mediante voto electrónico: la utilización de software libre y la emisión de un comprobante en papel, del voto, emitido en forma electrónica.

Sobre la utilización de un software libre, Romero Flores y Tellez Valdez (ROMERO FLORES Y TELLEZ VALDEZ, 2010) sostienen: "La premisa básica para considerar a un software libre de uno que no lo es, consiste en que los usuarios están autorizados para estudiar el funcionamiento del programa o sistema, adaptarlo a sus necesidades y estar en condiciones de distribuirlo, incluso produciendo programas derivados, aunque no necesariamente la condición de libre implica gratuidad ya que existen condiciones para su utilización". Boltz y Centeno Laopas (Boltz y Centeno Laopas, 2005) amplían esta idea: "Quienes adhieren a esta postura consideran que este procedimiento resulta mejor en la tarea de adaptación o modificación del software, arreglar fallas operativas de seguridad, y verificar su funcionamiento interno sin depender de un único proveedor".

Sobre la necesidad de contar con un comprobante en papel del voto emitido, Clemente (CLEMENTE, 2007), señala que: "La boleta electoral constituye el instrumento mismo con el cual el votante expresa su preferencia política", por ello es recomendable, que en el sistema de voto electrónico se mantenga la boleta, como comprobante tangible de la elección del votante.

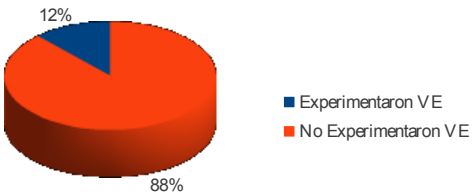
También, la boleta en papel es de vital importancia al realizar el escrutinio de votos ya que brinda la posibilidad de realizar un recuento manual de votos, evitándose la posibilidad de maniobras fraudulentas. Así, se otorga mayor confiabilidad al elector, que puede verificar su elección en el comprobante papel de su voto y también en el resultado del escrutinio, que no se basa tan sólo en un control electrónico.

A tal efecto, resulta aconsejable efectuar una adecuada regulación legislativa, que establezca, luego de finalizada la elección, en la oportunidad del escrutinio provisorio, la selección de una muestra de mesas electorales, por el método de muestreo aleatorio simple estratificado (esto es, definiendo los estratos en función de la cantidad de votantes por distrito), de manera de poder llevar adelante un recuento manual de las mesas seleccionadas y evaluar si el margen de error es aceptable o no. Esta selección aleatoria, debiera realizarse una vez finalizados los comicios, a modo de evitar que dichas mesas hayan funcionado ¨intencionalmente bien ¨y que ello pueda llevar a la conclusión, que todos los comicios se desarrollaron dentro de los parámetros esperados.

III
EL VOTO ELECTRÓNICO EN EL MUNDO

El sistema de voto electrónico ha sido implementado en varios países del mundo, según informa el portal del país Vasco, 7 han adoptado el voto electrónico, 5 lo probaron y lo prohibieron y 19 están en un proceso de estudio y prueba.

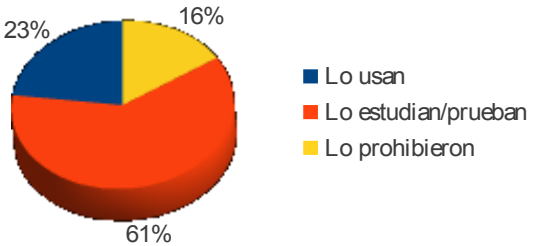
Gráfico I Estado del VE en el Mundo



El voto electrónico emergió como algo más confiable que el método tradicional, en función de una creciente desconfianza en la política y las instituciones por parte de la comunidad. Si bien las experiencias solo se han realizado en casi el 20% de los países del mundo, y no todas han sido exitosas puede preverse que este será el sistema electoral en un futuro no muy lejano.

Entre los países fuera de Latinoamérica, en los que se encuentra vigente el voto electrónico, se encuentran: Bélgica, Estonia, Filipinas, La India y Estados Unidos. Su uso, solucionó problemas relacionados con territorios muy extensos y gran cantidad de población (por ejemplo India).

Gráfico II
Resultados de las Experiencias sobre Voto Electrónico



- En otros países se ha prohibido el uso del voto electrónico, como es el caso de Holanda y Alemania, donde se generó un importante rechazo hacia el sistema debido a una gran desconfianza en la transparencia de las nuevas tecnologías. Para analizar las experiencias en los distintos países debemos dividir sus experiencias en dos categorías:
- La urna electrónica donde el votante se encuentra físicamente supervisado por representantes del órgano electoral encargado de los comicios.
- El voto remoto, en el cual el votante emite su voto mediante la telefonía celular o Internet.
- El mecanismo electrónico más utilizado por quienes han decidido incorporar nuevas tecnologías a sus sistemas de votación es la urna electrónica, y aunque estos modelos varíen entre países, los sistemas son esencialmente los mismos, es decir, una combinación del equipo electrónico o electromecánico usado para emitir y contar votos, y que mantiene y produce un rastro de información auditable. Este tipo de ins-

trumentos tecnológicos se han probado, con mayor o menor fortuna, en muchos países desarrollados y algunas de las mayores democracias del mundo.

III.1.- SISTEMAS DE URNA ELECTRÓNICA

III.1.1.- Alemania

En Alemania la votación a través de urnas electrónicas había sido utilizada por más de diez años. Sin embargo, la Corte Constitucional Federal Alemana declaró como inconstitucionales los sistemas electrónicos que fueron usados en las elecciones generales de 2005 y por ello no pudieron ser utilizadas en las elecciones de septiembre de 2009. La Corte sentenció que el uso de máquinas electrónicas contradice la naturaleza pública de las elecciones, además de que el equipo utilizado en 2005 tuvo carencias. Sin embargo, dado que no hay evidencia de errores ocurridos en el pasado, los resultados de elecciones previas permanecerán validos; otra razón fundamental para tomar esta medida fue que las máquinas de votación electrónica no ofrecían un comprobante escrito que le permitiera al elector verificar la opción elegida, lo cual requería que los usuarios confiaran totalmente en la tecnología.

El fallo donde el Supremo Tribunal Constitucional (CORTE CONSTITUCIONAL ALEMANA, 2009) prohibió la utilización del voto electrónico se sustentó en el "principio de publicidad de las elecciones", según el cual todos los pasos esenciales de la votación deben estar sujetos al control público. Según el Tribunal: "… los votos no pueden quedar depositados exclusivamente en una memoria electrónica. El votante no puede ser remitido, luego de la

votación electrónica, a confiar exclusivamente en la integridad técnica del sistema.-…

…El legislador no está impedido de utilizar aparatos electorales en elecciones, si se ha asegurado la posibilidad constitucional de un control de corrección confiable. Especialmente son imaginables aparatos electorales en el que los votos se registren, no sólo en la memoria electrónica. Esto es posible por ejemplo, en aparatos electrónicos que además del registro electrónico del voto imprimen un protocolo de papel visible, que puede ser controlado antes de la emisión del voto definitivo y que es recolectado para posibilitar una verificación.¨ (Fallo de la Corte Constitucional Alemana -2BvC 3/07 – 2BvC 4/07-, pronunciada el 3 de marzo de 2009 en el proceso de Queja de Control Electoral contra la resolución del Bundestag Alemán del 14 de diciembre de 2006, Justicia Electoral, Revista del Tribunal Electoral del Poder Judicial de la Federación, Cuarta Epoca, Vol. I, núm. 6, 2010, México, diciembre de 2010, p.509/568. Traducción de Manfredo Koessl, con nota de José M. Pérez Corti).

Con este fallo, la Corte ha sostenido que la introducción de urnas electrónicas por parte de la Ordenanza Federal sobre máquinas de voto fue inconstitucional, debido a que no se aseguró que las máquinas que se aprobaron y usaron en las elecciones cumplían con los requisitos constitucionales y respetaban principios fundamentales a la naturaleza pública de las elecciones, además de que dificultaban la detección de manipulación malintencionada o accidental de los procesos, que ocasionaría un funcionamiento equivocado de los procesos de votación.

Aún así, podemos concluir que el Tribunal no se pronunció en contra de las máquinas electrónicas de votación, sino en cuestiones reglamentarias relacionadas con el poder de policía electoral y de ejecución. Concretamente respecto a cuestiones que se relacionan con un adecuado control de los comicios y de sus resultados por parte de los ciudadanos y de las autoridades electorales. Si bien este tema será revisado por el gobierno alemán para continuar mejorando sus sistemas electorales, hasta el momento la prohibición de la utilización de las urnas electrónicas continúa, pero mientras tanto observaría los avances en votación electrónica a nivel internacional.

III.1.2.- Australia

En este país, se ha utilizado el voto electrónico para que emitan su voto los miembros de sus fuerzas armadas en el extranjero. También, se utilizó como herramienta para permitirles a personas con problemas visuales expresar su voluntad política. Para 2003, el sistema electoral australiano ya había diseñado un sistema de código abierto a través de una compañía australiana privada, con especificaciones dadas por oficiales electorales, quienes hicieron público el código a través de Internet, para ser evaluado por la ciudadanía.

El sistema fue desarrollado en seis meses y utilizado en una prueba piloto durante las elecciones de 2001, y se hizo especial hincapié en que su diseño se ajustó a las especificaciones del gestor electoral. Aunque, actualmente, esta tecnología se encuentra a prueba, en 2007 los australia-

nos con capacidades visuales diferentes pudieron emitir sus votos a través de máquinas de votación electrónica en la elección federal. En el 2002, la Comisión Electoral Australiana recomendó, al Parlamento Federal, realizar ejercicios electorales vinculantes, en sus próximas elecciones.

En 2001, se realizó la primera experiencia piloto en Canberra utilizando el sistema EVACS (Electronic Voting And Counting System) el que fue nuevamente utilizado en las elecciones de octubre de 2004.

En 2006, en las elecciones parlamentarias en el estado de Victoria, se instalaron 37 terminales en seis colegios, con el fin de facilitar el voto a las personas con discapacidades visuales y a aquellos votantes con dominio limitado del inglés. En 2007, en las elecciones federales la Comisión Electoral Australiana puso 29 puestos de votación electrónica, lo cual permitió votar a electores con discapacidad visual, en un periodo previo y durante la jornada electoral.

Sin embargo, para el 2009, debido a los costos incurridos en la implementación de este sistema de ayuda para los ciudadanos ciegos, el Comité Bicameral Permanente sobre Asuntos Electorales ordenó discontinuar los pilotos para evaluar los programas. En 2010, el estado de Victoria utilizó puestos de votación electrónica para electores con discapacidad visual y centros de votación móviles para electores hospitalizados y ancianos.

III.1.3.- Bélgica

Empezó en 1989, así el gobierno belga fue pionero en la aplicación de sistemas de voto electrónico. El método

se basaba en tarjetas de banda magnética los datos se grababan con la ayuda de una pantalla táctil y un lápiz óptico. Posteriormente se introducían las tarjetas en urnas electrónicas, que computaban automáticamente los resultados. En 1994, se estableció el marco legal para el voto electrónico.

En el 2010, comenzó un proceso de licitación para la selección de un nuevo sistema. El nuevo sistema, se basa en una urna electrónica con pantalla táctil y con posibilidad de imprimir un comprobante del voto en papel, para posibles auditorías de los resultados electrónicos. En 2014, durante las elecciones al Parlamento Europeo Regional y Federal, se usó un sistema de voto electrónico totalmente automatizado y verificable. Sin embargo, un fallo informático obligó a anular 2.200 votos que representaba el 0,06% del total.

III.1.4.- Emiratos Árabes Unidos

En 2006, se realizó la primera experiencia con voto electrónico en las elecciones del Consejo Nacional Federal. En 2011, para las elecciones nacionales se desplegaron, en 13 grandes centros de votación, 700 máquinas de votación con pantallas táctiles y 320 estaciones de identificación.

III.1.5.- España

- En las elecciones para el parlamento Europeo de junio de 2009, se presentó el Colegio Administrado Electrónicamente (CAE), el cual sería puesto a prueba en las ciudades de Lleida, Pontevedra y Salamanca, que representó 154 colegios electorales, 459 mesas y 280.520 electores. Este método de

votación electrónica, dotaba a los funcionarios de las mesas electorales con herramientas informáticas que facilitaban sus funciones. Constituida por una computadora tipo laptop, una impresora, un lector óptico y una memoria USB, que lleva encriptada la lista electoral de cada mesa, según la Oficina del Censo Electoral. Al inicio del la elección, el presidente de mesa enciende el ordenador y pone en marcha una aplicación, que permite a los miembros de la mesa, realizar las gestiones que conllevan un proceso de votación:

- Tener acceso a la información almacenada en el USB, que se encripta de forma automática.
- Confeccionar en el ordenador el acta de constitución de la mesa.
- Llevar el control de los electores a través del Documento Nacional de Identidad (DNI), que en caso de ser electrónico se utiliza un lector óptico para registrar su participación, o en caso de ser tradicional se busca manualmente en la lista electoral.

Llevar a cabo el recuento de los votos a través del lector óptico, incluyendo aquellos votos enviados por correo y los que fueron emitidos dentro de la mesa, y al finalizar.

Se completan las actas correspondientes sin errores, se redactan las incidencias y se envían los datos al Centro de Recepción de Información.

- El Colegio Administrado Electrónicamente ofrece una multitud de ventajas: garantizar la seguridad, debido a que elimina los errores de transcripción; es más eficaz, porque facilita la localización de los

electores en el censo, y el proceso de recuento y envío de datos, lo cual hace que el proceso sea mucho más rápido, y es más ecológico y barato por el papel que ahorra. Las diversas experiencias piloto realizadas a nivel de Comunidades Autónomas y Estado son:

- País Vasco: En 1998, fue pionero en la regulación del voto electrónico para las Elecciones al Parlamento Vasco. El Gobierno Vasco desarrolló su propio sistema de voto electrónico denominado Demotek, que fue utilizado en diversos procesos electorales, como las elecciones en la Universidad del País Vasco, del Athletic Club de Bilbao y una prueba piloto en las elecciones al Parlamento de europeo.
- Catalunya: En 1995, se desarrolla una experiencia en dos colegios electorales en las elecciones al Parlamento de Catalunya con tarjetas de banda magnética. En 2003, en las elecciones al Parlamento de Catalunya se realizó una prueba piloto de voto electrónico remoto, para los electores catalanes residentes en el extranjero (Argentina, Bélgica, Estados Unidos, México y Chile). También, se experimentó en estas elecciones con dos sistemas diferentes de voto electrónico presencial, en cinco municipios: uno el sistema Demotek del Gobierno Vasco y otro de una empresa privada mediante pantalla táctil. En 2010, el Ayuntamiento de Barcelona realizó una consulta ciudadana, en la que utilizó votación electrónica a través de Internet o telefonía móvil. Se registraron numerosos problemas.

- Galicia: En 1997, en las elecciones al Parlamento de Galicia, se probó en dos mesas electorales dos sistemas: uno francés y otro japonés, los dos con pantalla táctil. En 2005, en las elecciones al Parlamento de Galicia, tuvieron lugar dos pruebas de voto electrónico con pantalla táctil.
- Comunidad Valenciana: En las elecciones autonómicas de 1999, se desarrolló en Villena (Alicante) una experiencia del voto con el sistema de votación electrónica francés CIVIS, que utiliza banda magnética, en la totalidad de las 39 Mesas electorales.
- Andalucía: En 2004, se efectuó en el municipio de Junta una prueba de voto electrónico a través de Internet.
- Estado Español: En las elecciones generales de 2004, se realizó la primera prueba de voto electrónico remoto en tres mesas. En 2005, con ocasión del referéndum de la Constitución Europea, se realizó un ensayo de voto electrónico remoto por Internet, sin validez, días previos a las elecciones, en un municipio de cada una de las provincias. La participación fue escasa. En las elecciones a Diputados y Senadores de 2008, en las Europeas de 2009, y en las Municipales de 2011 (también en las Autonómicas de Cataluña de 2010), se experimentó en diversas poblaciones, a instancias del Ministerio del Interior, el sistema de la Mesa administrada electrónicamente, que consiste en la automatización de las tareas más importantes de las Mesas Electorales.

III.1.5.- Finlandia

El proyecto de reforma realizado en el Sistema de Información Electoral de Finlandia, planeó introducir el voto electrónico en las casillas electorales. El experimento fue realizado en 2005 como un proyecto piloto, para ello se modificó el documento que corrige el Acuerdo Electoral, que tuvo efecto desde enero de 2007 a diciembre de 2008, en las elecciones municipales de 3 municipios. Los ciudadanos, que estaban en condiciones de votar, dentro de estas tres municipalidades, tuvieron la oportunidad de sufragar electrónicamente en las casillas electorales de avance general y en las casillas electorales el día de los comicios.

El voto electrónico se planeó como una alternativa a los métodos tradicionales de boleta de papel, lo cual significa que en una fase inicial también será posible votar utilizando la boleta tradicional. Sin embargo, la meta es implementar un sistema de voto electrónico en el 100% de las casillas de todas las elecciones. Además, se pretende crear un sistema que sea suficientemente amistoso con el usuario como para que cualquier persona lo pueda utilizar, operando, bajo el principio básico con el cual funcionan los cajeros automáticos, con la única reserva de que no se necesita una tarjeta electrónica para la identificación del usuario.

El sistema finlandés sostiene principios centrales para llevar a cabo elecciones seguras utilizando sistemas que se basan en soluciones tecnológicas. Se registran el voto y la identidad del usuario, las cuales se registran en

una urna electrónica a través de una terminal de voto utilizando un sistema de encriptando de datos que mantienen separados la identidad y el voto. El sistema electrónico implementado en Finlandia, es desarrollado por una compañía del sector privado, la cual usa un sistema de seguridad informática llamado Pnyx.core, creado por una empresa de software española.

III.1.7.- Francia

En 1969, el Código Electoral francés autoriza el uso de máquinas electrónicas. Entre 2000 y 2002, se realizaron diversas pruebas de voto electrónico en paralelo al voto tradicional. En 2003, se realizó una de las primeras votaciones por Internet permitiendo a los ciudadanos franceses residentes en Estados Unidos la renovación del Consejo Superior de los Franceses en el Extranjero.

En 2005, el Ministerio de Interior aprobó el uso de un nuevo sistema de voto electrónico, basado en pantalla táctil, que fue usado en el referéndum sobre la Constitución Europea.

En las elecciones presidenciales de 2007, el 3% de los votantes registrados utilizaron urnas electrónicas para emitir el sufragio. Se utilizó un sistema de votación electrónica en 82 localidades, y en algunos casos mostraron largas filas, fallas de los sistemas y abandono total de ciertas poblaciones; algunos partidos políticos denominaron el ejercicio como una catástrofe, demandando que se retiraran las urnas electrónicas para la segunda ronda de la elección presidencial. Incluso hubo un estudio realizado por la Universidad de Nantes que encontró diferencias entre casillas

donde se utilizaban las boletas de papel y en aquellas que utilizaban urnas electrónicas: existían inconsistencias de firmas de actas y conteo de votos en 29.8% de las casillas con urnas electrónicas en comparación con sólo 5.3% de casillas tradicionales. Este tipo de controversias suscitaron muchas críticas al proceso electoral, sin embargo, al final, la elección determinó como ganador a Sarkozy, siendo ratificado por el Congreso francés a pesar de las acusaciones de sus opositores. La Unión Europea ha presupuestado 3.2 millones de euros para iniciar un programa piloto de tres años, donde se utilicen medios electrónicos, para realizar elecciones en cuatro diferentes locaciones: una en Francia, dos en Alemania y una en Suecia. En 2012, los franceses en el extranjero pudieron votar durante seis días a través de Internet, para las elecciones a la Asamblea Nacional. El número de electores que utilizaron el voto electrónico fue de 127.000.

III.1.8.- Holanda

El resultado de la utilización del voto electrónico en Holanda fue controversial. Este tipo de tecnología fue aprobada en 1997 y era utilizada desde entonces. Sin embargo, en 2006, una comisión investigadora encontró, que las urnas utilizadas en los Países Bajos podían ser fácilmente alteradas y modificadas en sus cómputos parciales. Como resultado, en las subsecuentes elecciones legislativas del 22 de noviembre de 2006, se prohibió la utilización de las urnas electrónicas en 25 ayuntamientos. Para el año siguiente, el Tribunal de la Corte de Distrito de Ámsterdam retiró la certificación de las máquinas electorales y finalmente en 2008, el gobierno holan-

dés prohibió por completo su uso. Actualmente, todas las elecciones en este país se realizarán a través de boletas de papel y lápices de color rojo, de acuerdo al reporte de la Organización para la Seguridad y la Cooperación Europea. Actualmente Holanda está interesada en el desarrollo del voto por teléfono y a través de Internet.

III.1.9.- India

La India es un ejemplo de la efectividad en el uso de las tecnologías, sobre todo, tomando en cuenta que es un país en vías de desarrollo. En 2004 más de 680 millones de personas emitieron su voto a través de un millón de dispositivos electrónicos sin que los resultados de la elección fueran motivo de controversia, lo cual fue considerado como una experiencia exitosa. El padrón electoral indio consiste en una lista de ciudadanos constituido por la Asamblea de Votantes y dividida en partes que corresponden a casillas electorales. La Comisión Electoral de la India ha decidido tener un máximo de 1200 electores por casilla, y el elector no debe de residir a más de 2 kilómetros de la casilla que le corresponde. Este organismo ha dictaminado, que la identificación del votante sea obligatoria. Se hace énfasis, en la dualidad de la identificación del elector y su debido registro en el padrón electoral. El incumplimiento de uno de estos dos factores inhabilita al elector de su capacidad para votar; esto indica que el padrón electoral y la emisión de la tarjeta son dos elementos que no necesariamente están relacionados y representa un trabajo doble; levantar el censo y construir la base de datos de las tarjetas. Esto supone un doble candado, pues hay que estar registrado

oficialmente en el censo y además realizar los trámites para obtener la tarjeta. La elección de 2004 duró cuatro semanas y requirió de más de 6.5 millones de colaboradores oficiales durante los comicios, el 60% de la población elegible participó en las elecciones, lo cual dota de mayor legitimidad al proceso.

La urna electrónica está diseñada para que no puedan alterarse de forma externa los cómputos de las casillas. Asimismo, cuando un voto es emitido se realiza una pausa de doce segundos antes que el sistema se reinicie y pueda contar el siguiente voto. Cuando se intenta forzar a la máquina para que cuente más rápido, esta se desconecta, lo que ayuda a evitar distorsión en el conteo o algún tipo de fraude. Las casillas no están conectadas a Internet, y la suma de votos se ubica en una memoria externa que sólo se puede decodificar en las oficinas centrales del órgano electoral. Los datos solamente se pueden codificar e imprimir por medio de una orden federal, y el código fuente, bajo el cual opera, está incrustado en un microprocesador, impidiendo que este sea reprogramado; el aparato es manufacturado en su totalidad por compañías propiedad del Estado.

Un grupo de académicos de la Universidad de Michigan y de personas de una empresa privada, lograron hacerse de un dispositivo de votación electrónica de la Comisión Electoral de la India. En su estudio, demuestran varias debilidades que tiene el sistema debido a cuatro fallas:

- El hardware del aparato es extremadamente sencillo, por lo cual se pueden fabricar dispositivos que

alteren los resultados de las elecciones si se tiene acceso privado al dispositivo de control.

- El código fuente bajo el cual opera la máquina, no está encriptado.
- Su funcionamiento no puede ser verificado una vez que el dispositivo se pone en marcha.
- Carece de un registro verificable de papel.
- Se ha exigido que dichos estudios, sobre la vulnerabilidad de los sistemas electrónicos, sean presentados ante el Comité Técnico Experto de la Comisión Electoral de la India, pues de lo contrario sólo constituye una campaña de propaganda para desvirtuar el sistema, y causar una polémica mediática con tintes políticos.
- El sistema electrónico utilizado en la India está compuesto por dos elementos: el dispositivo de control y el dispositivo de votación. De este modo, cada boleta puede ofrecer hasta 16 opciones diferentes, pero cada aparato puede controlar varias boletas a la vez, dado el caso que se necesiten más opciones. Sin embargo, un dispositivo de votación electrónica que ha sido capaz de registrar elecciones de la democracia más grande del mundo, merece ser estudiado por su funcionamiento, practicidad y economía. Su procedimiento es bastante sencillo y al parecer, todos los países que utilizan, de manera vinculante, los sistemas de votación electrónica están siguiendo protocolos muy similares:
- Primero, el oficial de casilla muestra a los repre-

sentantes y demás observadores, que la casilla ha sido puesta en ceros.

- Al oprimir un botón en la máquina que emite un conteo de los votos almacenados.
- Una vez que ha empezado la elección, los electores oprimen un botón colocado junto al nombre del candidato de su preferencia, lo cual hace, que la máquina emita un sonido que indica que el voto ha sido registrado.
- Al terminar la elección, el oficial de la casilla oprime un botón que hace que la casilla se cierre, y en ese momento se imprime el recibo con el conteo final de los votos.

Estas máquinas fueron puestas a prueba en diversos lugares de la India, se llevaron a cabo campañas publicitarias en los medios masivos de comunicación, seminarios académicos conducidos por la Comisión Electoral de la India en varios foros, y se dispuso de métodos de retroalimentación para afinar el desempeño de la máquina. El aparato utiliza un microprocesador que tiene un código PROM que almacena los datos introducidos, el cual no puede ser retirado ni alterado. Este código ha sido revisado extensamente para liberarlo de todo error, además de utilizar almacenamiento de memoria de doble redundancia, que guarda la información sin necesidad de una batería de respaldo. Todas las unidades son selladas para asegurarse que no son alteradas.

Las elecciones de 2004 fueron llevadas a cabo utilizando un millón de máquinas de votación electrónica, cuyo precio unitario oscila en los 300 dólares. Sin em-

bargo, el ahorro a largo plazo se estima en unas diez mil toneladas de papel por cada elección. Cada máquina puede almacenar hasta 4000 votos, y emiten resultados oficiales en las 24 horas posteriores a la elección.

III.1.10.- Irlanda

En 2000, se modificó la legislación para la introducción del voto electrónico. En 2002, se realizó la primera prueba en las elecciones generales entre los ciudadanos de Dublín Norte, Dublín Oeste y Meta. En el sistema, el votante selecciona el botón de los candidatos en el orden de preferencia que desea, mediante un tablero electrónico dotado de una pantalla. En 2004, el gobierno irlandés creó una comisión independiente para evaluar la seguridad y confidencialidad del voto electrónico. La comisión examinó la insuficiente seguridad y concluyó que no garantizaba la integridad de la elección. En 2009, el gobierno anunció suspender la introducción del voto electrónico, tanto por los costes económicos que exigía su implantación, como por la satisfacción que el electorado tenía en el sistema de votación tradicional. En 2012, el gobierno decidió deshacerse definitivamente de 7500 máquinas electrónicas adquiridas en el 2002 por falta de fiabilidad.

III.1.11.- Japón

El sistema electoral japonés requiere que los votantes escriban el nombre de su candidato, o partido preferido, sobre una boleta en blanco dentro de la casilla el día de las elecciones. Este sistema se ha utilizado por más de 100 años, desde el establecimiento de un sistema moderno de elecciones en este país. Esto deja en desventaja

a las personas analfabetas y/o discapacitadas. Por esta razón, se ha modificado la Ley Electoral con la adición de un complemento que versa sobre la votación y las máquinas de votación para el registro electromagnético con referencia a la elección de los miembros del Consejo y de los jefes de los gobiernos locales. La primera prueba piloto fue organizada en la municipalidad de Kawaguchi en 1999, con 59.943 participantes, a través de 78 casillas. La primera ciudad en implementar el sistema electrónico en Japón a través de un ejercicio vinculante fue la ciudad de Niimi, en la prefectura de Okayama, en junio de 2002. Esta pequeña ciudad, rodeada por las montañas Chugoku, cuenta con una población de 25.000 habitantes. El gobierno local envió una propuesta de integrar el voto electrónico para sus elecciones en febrero de 2001, la cual promovió la ley, que se aprobó en marzo de 2002; una vez que esta ley especial entró en vigor, la asamblea de la ciudad aprobó una reglamentación a nivel local, que hace frente a los medios de almacenamiento electromagnético para registrar el voto.

El sistema es bastante sencillo:

- Al llegar el elector a la casilla, se le identifica y se le entrega una tarjeta con la cual puede acceder a la interfaz de la máquina.
- Una vez utilizada la tarjeta, el elector opera la máquina para elegir un candidato, y su voto es almacenado en un medio de almacenaje.
- Al salir de la casilla, el elector debe entregar la tarjeta a la persona responsable. Se puede decidir si

estas tarjetas se protegen para no poder ser recicladas en la misma elección.

El dispositivo de votación electrónica fue desarrollado por la Asociación de Sistema Electrónico de Voto: tiene una pantalla táctil de 15 pulgadas, el cual permite un funcionamiento muy similar al de un cajero automático.

Esta elección arrojó resultados 25 minutos después de haber cerrado las casillas, lo cual demostró lo fácil y cómodo que es el sistema. En total fueron utilizados 103 dispositivos en 34 estaciones de votación, donde había hasta 7 dispuestos en fila. La ley, que hace frente a los casos especiales, para utilizar un método de votación que use un tipo de almacenaje electromagnético para la elección de miembros de las asambleas y los oficiales ejecutivos en jefe de entidades públicas, fue aprobada en 2001, se llamó Ley Especial de Votación Electrónica, esta ley provee a las elecciones locales con la opción de utilizar dispositivos de voto electrónico, como un caso especial contemplado dentro de la Ley de Elecciones de Oficinas Públicas, la cual provee los lineamientos, para las elecciones de los miembros del régimen, los miembros de las asambleas y los oficiales ejecutivos en jefe, de los gobiernos locales. La ley establece, que la votación electrónica sólo podrá ser utilizada el día de la jornada electoral, y no para el voto anticipado, el voto en braille, y el voto por correo tradicional, además que provee la posibilidad de asistencia a aquellas personas con capacidades diferentes, que no pueden emitir un voto por ellos mismos, haciendo especial hincapié en que el voto sea emitido, exclusivamente, por el elector al cual pertenece dicho voto. En 2004, se instauró un procedimiento, que

permitía a los ciudadanos japoneses votar por adelantado, lo cual fue usado por el 11% de la población electoral.

Una de las críticas, más sustanciales al dispositivo japonés de votación electrónica, es el tamaño de su pantalla, ya que no permitía mostrar muchos nombres de candidatos al mismo tiempo, aun así la población acogió con gusto el nuevo sistema, porque lo consideran, un paso hacia delante de su sistema tradicional de voto en la mano.

III.1.12.- Kazajistán

En 2004, realizó sus primeras experiencias de voto electrónico en las elecciones parlamentarias. En 2005, en las elecciones realizadas en varios distritos de la ciudad de Taldykorgan, se utilizó el sistema de voto electrónico denominado "Sailau". En 2007, en las elecciones parlamentarias se volvió a utilizar el voto electrónico, pero días anteriores dos expertos ponían en duda la seguridad del sistema. En 2011, la Comisión Electoral Central se abstuvo de usar el sistema de voto electrónico "Sailau", ya que los electores expresaban sus sospechas sobre falsificaciones.

III.1.13.- Noruega

- En 2011, se utilizó por primera vez el voto electrónico en 10 municipios, presentándose como un medio alternativo del voto tradicional. El ciudadano tuvo la posibilidad de elegir entre ambos. En esas elecciones, el 22% emitió su voto anticipado en un periodo de treinta días previos a la fecha de la jornada electoral; de los cuales 73% de ellos utilizaron medios electrónicos. Para lograr esto, fue

necesario realizar una reforma electoral, para adicionar o aclarar ciertos aspectos del proceso electoral no contemplados en la legislación anterior; utilizando la autoridad, que el Ministerio tiene sobre la Ley Electoral para establecer las directrices, de tal manera que se permita llevar a cabo elecciones que utilicen sistemas de tecnología digital, respetando los principios que todo proceso electoral democrático debe tener. Es por esta razón que se estipula lo siguiente:

- El voto electrónico, sólo es utilizado como un complemento a la votación en la mesa de votación.
- El voto electrónico, sólo es válido durante el periodo de votación anticipada, y no durante la jornada electoral.
- Un elector, que haya emitido su voto durante el periodo de votación anticipada, puede corregir su voto el día de la jornada electoral.

Un voto, emitido en una boleta tradicional de papel, anula un voto electrónico.

El sistema electrónico es seguro y fiable, por lo cual el vínculo entre el voto y el elector nunca se revela. El Ministerio de Interior noruego, estipuló que las bases normativas de la ley electoral se aplican, a menos que se determine lo contrario, en el reglamento especial para la votación electrónica, esto sin violar los principios básicos.

III.1.14.- Rusia

Rusia introdujo diferentes herramientas tecnológicas en sus procesos electorales, desde hace casi once años.

El sistema es conocido como Vybory y ha ido cambiando para abarcar cada vez más áreas del proceso democrático. Desde la etapa de planificación de la elección, el registro electrónico de los votantes, el monitoreo del uso de los recursos gubernamentales durante las campañas, hasta la emisión y conteo del voto en casillas sensibles al tacto, Rusia ha ido desarrollando uno de los sistemas de votación electrónica más sólidos y confiables a nivel mundial. Una de las claves, ha sido la paulatina introducción de la tecnología, en el proceso a través de un sistema de ensayo y error, para ir corrigiendo y mejorando las estrategias y herramientas utilizadas en los ejercicios democráticos. Actualmente, la Comisión Electoral Central de este país, planea utilizar cerca de 3000 máquinas de votación electrónica en 20 de los territorios de este país durante las siguientes elecciones regionales, desde el extremo europeo hasta Siberia.

III.2.- SISTEMAS CON USO DE LA TECNOLOGÍA CELULAR

III.2.1.- Canadá

En las elecciones federales se sigue utilizando el voto tradicional mediante papel. La votación electrónica se ha usado a nivel municipal. Cada provincia y cada municipio puede elegir sus propias máquinas de votación y las normas de votación, aunque hay municipios que deben seguir las normas y reglamentos provinciales En 1995, se realizó la primera votación municipal con voto electrónico en la ciudad de Winnipeg.

Internet ha sido utilizado para llevar a cabo varias elecciones en Canadá a nivel local, Markham, Peterbo-

rough y Halifax son localidades donde se ha usado el voto remoto por Internet, para estudiar el potencial, que tendría un sistema de voto a través de la tecnología digital. Seis, son las provincias, que han aprobado una legislación como parte del Acuerdo de Elecciones Municipales, el cual permite a los municipios implementar formas alternativas de voto, o alguna forma de voto electrónico, o bien, aprobar una ordenanza municipal que autorizaría el uso de métodos alternativos de sufragio. El voto por Internet ya ha sido usado activamente en elecciones canadienses, pero sus efectos sólo fueron a nivel local. La primera experiencia se llevó a cabo en 2003, en el pueblo de Markham, en seis municipios en Stormont, Dundas y Glengarry, y en cinco municipalidades en Prescott-Russell. En 2006, Markham y Peterborough usaron la Internet en sus elecciones municipales, así como ocho pueblos a través de Ontario, los cuales también ofrecieron voto por teléfono celular. En 2008, Halifax, y los pueblos Novoescoceses de Berwick, Windsor, y Stewiacke, llevaron a cabo sus elecciones municipales y de consejo académico de las escuelas locales, incorporando el voto por Internet y por teléfono celular como un método de votación alternativa, y Halifax recientemente implementó una expansión de esa estrategia en una elección, que llevó a cabo el 19 de septiembre de 2009.

Las tres comunidades más prominentes, que introdujeron programas de votación electrónica, muy diferentes entre sí son: Markham es una localidad urbana, tiene más alto nivel de ingresos entre sus residentes y es uno de los municipios más grandes en el Área Principal de Toronto,

además de tener un mayor acceso a la tecnología. Halifax, aunque es la más urbana y desarrollada de los municipios de la costa atlántica, todavía tiene áreas carentes de desarrollo, de las cuales algunas apenas están adquiriendo acceso a Internet; su electorado es mayor que el de Markham, está localizado en una región geográfica diferente en el país, y tiene figuras demográficas contextuales muy contrastantes. El electorado de Peterborough es menos urbano, y sus residentes tienen un ingreso menor en promedio. A pesar de estas diferencias culturales y demográficas, la introducción del voto electrónico fue bien recibida por el público en las tres comunidades, y aparentemente los residentes están dispuestos a verse inmersos en procesos similares en el futuro. En total, Canadá debe de realizar ocho pasos para instaurar efectivamente un sistema de votación electrónica como ellos lo han diseñado:

- Asegurar el acceso universal a la tecnología.
- Obtener una cultura de apoyo por parte de todos los actores políticos.
- Fijar un marco legal, que provea las necesarias instancias para implementar métodos alternativos de votación electrónica.
- Llevar a cabo una investigación profunda sobre los resultados obtenidos, en todas las jurisdicciones electorales.
- Establecer claramente las metas que se desean obtener mediante el voto electrónico.
- Llevar a cabo una apropiada campaña de marketing y publicidad.

- Establecer un sistema de prácticas y pruebas graduales para sensibilizar a la población.
- Utilizar pruebas de evaluación para asegurar, que el método está obteniendo los objetivos deseados.
- En 2011, seis provincias (Alberta, Columbia Británica, Nueva Brunswick, Nueva Escocia, Ontario y Quebec), aprobaron leyes que permiten diversas formas de voto electrónico incluido el voto por Internet.

III.2.2.- Corea del Sur

El problema de Corea del Sur es cómo facilitar, efectivamente, la deliberación política y cómo incrementar la participación electoral a diferentes niveles, para profundizar la democracia en el país. Entre las diversas medidas que va a adoptar el país, el voto electrónico es considerado como el instrumento más moderno para el desarrollo de la democracia participativa y deliberativa.

Un factor importante para la rápida recuperación de la crisis económica que Corea del Sur sufrió en 1997, fue la implementación de instituciones democráticas de alta calidad que han florecido y han sido sostenidas por la consolidación de un régimen civil a principios de la última década del siglo anterior. Presenta un gran contraste con otros países asiáticos como Tailandia, Indonesia y Filipinas, donde las instituciones democráticas y los procesos electorales todavía son débiles y vulnerables. Aunque, han tenido muchos problemas en el pasado, la mayoría de los sudcoreanos tienen un fuerte apego a sus elecciones y a los resultados que de ellas emanan.

En enero de 2005, la Comisión Nacional Electoral de Corea del Sur anunció un plan maestro para implementar el voto electrónico, para hacerlo desde ese año en diferentes elecciones a diferentes fases. Este plan tiene como meta final, que los usuarios puedan votar desde cualquier lugar a través de Internet y los servicios de telefonía celular. En caso de ser exitoso, Corea del Sur pertenecerá al puñado de países que implementen un sistema de voto electrónico total, a nivel nacional.

En Corea del Sur, sus servicios de telefonía celular tienen una cobertura impresionante, y la integración que los teléfonos celulares han tenido en la vida de las personas excede cualquier medio de comunicación: desde movilizaciones sociales, pasando por mercadotecnia de todo tipo, y para 2012 incluyeron la posibilidad de emitir su voto a través de Internet. Sin embargo, existe la preocupación sobre la trivialización del voto, además de las debilidades de seguridad y el anonimato de éste; el voto por telefonía celular tiene sus méritos como una herramienta popular y de fácil alcance, aunque es posible que este medio no cumpla con los requisitos indispensables para garantizar elecciones seguras y anónimas. Durante la segunda mitad de la elección de 2005, para seleccionar superintendentes dentro de la oficina de educación por periodos de prueba, el CNE utilizó máquinas de voto electrónico de pantalla táctil, pero para las elecciones de la Asamblea Nacional, de 2008, mantuvo la boleta física junto con otros métodos convencionales de voto para las elecciones generales de 2012. Este sistema representa el trabajo de diez años de implementación paulatina, y una

vez finalizado el sistema, significaría un ahorro del 50% de los costos de montar una elección tradicional.

III.2.3.- Estonia

Este es uno de los países más identificados con los servicios de Internet y tecnología digital: la mayoría de sus ciudadanos pagan regularmente por los servicios de transporte y otros servicios menores de gobierno a través de sus teléfonos celulares; compran bienes y realizan transacciones bancarias a través de la red, e inclusive no hay rincón del país que no tenga cobertura de red inalámbrica. Con respecto a su democracia, Estonia es un país ejemplar. En solamente diez años, han pasado del comunismo a las aplicaciones avanzadas de la democracia electrónica. El voto electrónico ha pasado por un gran trabajo a través del Parlamento de Estonia, incluyendo la introducción de un estudio de seguridad por especialistas en criptología y trabajos holísticos por todos los cuerpos gubernamentales involucrados, incluyendo el Ministerio de Transporte y Comunicación, quienes se encargaron de los aspectos técnicos y logísticos de la operación: sus principales preocupaciones han sido la equidad de los ciudadanos en la vida política, la privacidad y el secreto del voto, la seguridad de los sistemas de voto electrónico, y cómo evitar el fraude electoral. En sus elecciones de 2007, uno de cada 30 ciudadanos emitió su voto a través de Internet, en lo que se convirtió, en la primera elección parlamentaria del mundo que permite votar a través de este medio. Para lograr esto, desde 2002 instauraron un nuevo sistema de identificación a través de una credencial electoral inteligente; con ella, un lector de

tarjetas, los controladores necesarios y una computadora, con acceso a Internet. Con lo anterior, el ciudadano puede ejercer su derecho a votar desde la comodidad de su hogar.

III.2.4.- Reino Unido

Las elecciones de 2001, tuvieron la participación electoral más baja de 90 años (59%), y ha invertido 30 millones de libras para incrementar las capacidades de adoptar sistemas de votación electrónica e implementando decenas de pilotos de prueba. El legado de la modernización electoral británica comienza con una revisión del Grupo de trabajo, sobre procedimientos electorales establecido por el gobierno en 1997: el trabajo de este grupo comenzó trazando los argumentos racionales para llevar a cabo la modernización electoral, y particularmente la introducción de voto por correo a petición, dentro del contexto del cuerpo legal del Reino Unido que históricamente siempre ha sido considerado como conservador; después evaluó el impacto de la modernización electoral, con específica atención en la evidencia concerniente a los beneficios y riesgos relativos asociados con el voto por correo, el voto electrónico y el conteo electrónico de votos.

El primer paso que dieron hacia la modernización de sus procesos electorales fue el Acuerdo para la Representación de los Ciudadanos de 2000, el cual proveyó la inmediata introducción del voto por correo a petición, así como el llevar a cabo pruebas de varias formas de voto electrónico. En diciembre del mismo año, se aprobó el Acuerdo de Comunicaciones Electrónicas, en el cual, se reconoció la legalidad de las firmas digitales y se autori-

zó a poner en marcha el servicio de votación electrónica para principios de 2001, que ha venido utilizando para asistir en las votaciones internas de diversas compañías. Finalmente, también en ese año se creó un cuerpo independiente denominado Comisión Electoral, el cual debería monitorear el proceso electoral y aconsejar al gobierno con respecto a la política electoral. A través, de estos dos acuerdos, en mayo de 2002, se aplicaron 16 pruebas de voto electrónico en los condados de Sheffield y Liverpool, con 20 más en el mismo mes del siguiente año, a nivel de autoridad local, que en todos los casos fueron ejercicios legalmente vinculantes. Lo que los pilotos quisieron evaluar fueron:

- Diferentes esquemas de conteo electrónico de voto.
- Sistemas de pantalla táctil.
- Voto por Internet y sistemas interactivos de respuesta a voz.
- Voto por teléfono terrestre.
- Voto por mensaje de texto SMS.

De un total de 174.000 votantes, un 40% eligió utilizar los medios electrónicos y el nivel de participación general aumentó en un 5.2%. Estas medidas obedecen a una preocupación por parte del gobierno británico por abatir el creciente abstencionismo y tratar de aumentar el voto joven. En estos comicios se eligieron representantes locales para el Congreso Europeo y formaron parte de un programa introducido por la oficina del primer ministro adjunto, que busca la eventual introducción del voto electrónico para las elecciones internas de Gran Bretaña. Actualmente, a través de esta iniciativa oficial se está modernizando la

base de datos del padrón electoral, ya que esta medida se contempla como un primer paso para la eventual aplicación generalizada del voto electrónico. El voto por televisión digital y el uso de tecnología dependiente en tarjetas inteligentes, para la identificación parcial de los electores fueron introducidas adicionalmente en 2003. Hasta 2007, el Reino Unido ha llevado a cabo más de treinta pruebas pilotos con diferentes sistemas de votación electrónica. En 2008, la Comisión Electoral declaró que con respecto a las pruebas realizadas, la seguridad y garantías adoptadas eran insuficientes y en consecuencia, determinó que no se continuaría con el voto electrónico.

III.2.5.- Suiza

Desde 1998, ha buscado implementar el voto electrónico para la organización de sus elecciones. La prueba piloto realizada en Ginebra, Neuchâtel y Zúrich, demostró, que el uso de la votación electrónica incrementa la participación de la ciudadanía, la calidad de la experiencia del voto, y es una aliada en la implementación de derechos políticos.

La historia del voto electrónico comenzó en febrero de 1998 cuando el Consejo Federal adoptó una "estrategia para una sociedad informática en Suiza". Esta tuvo dos metas importantes: la primera, fue instaurar una plataforma electrónica para todos sus servicios gubernamentales, y la segunda implementar un sistema seguro de votación electrónica no sólo para elegir gobernantes, sino para facilitar el ejercicio de otros derechos políticos que los ciudadanos suizos tienen, tales como firmar iniciativas, hacer referéndums, validar las listas de candidatos

para el parlamento y diseminar información sobre los votos y elecciones provista por las autoridades electorales.

En 2004, Ginebra introdujo su sistema de votación electrónica para una elección federal y cantonal, y se consideró un éxito, pues 21.8% de los votantes en las cuatro comunidades de Ginebra usaron el método electrónico, de una participación ciudadana del 56.4%. En noviembre del mismo año, se realizó una segunda prueba a nivel federal en ocho comunidades de ese mismo cantón. De una participación ciudadana del 41.1%, el 22.4% de los votantes lo hicieron de una manera electrónica. Es importante resaltar, que el método electrónico de votación utilizado en Ginebra es a través de Internet y no la urna electrónica. La idea de realizar las elecciones a través de la red es acercar el voto a los ciudadanos, para que la participación ciudadana se incrementara. En Zúrich, el proyecto de votación fue lanzado en 2002 en paralelo a los proyectos de Ginebra y Neuchâtel. La primera implementación en este cantón fue llevada a cabo en unas elecciones estudiantiles en la Universidad de Zúrich en 2004. Para 2005, el proyecto piloto fue extendido a las elecciones públicas de Bülach para un referéndum. En 2008, hubo votación electrónica disponible para 11 comunidades dentro del cantón de Zúrich. Cabe resaltar que la administración electoral es diferente para cada cantón, por lo tanto la implementación de sistemas de esta naturaleza también es diferente.

En Neuchâtel, se ha alcanzado la creación de una plataforma electrónica para la administración gubernamental del cantón y sus 62 comunidades. En esta plataforma

el ciudadano puede acceder a una variedad de servicios gubernamentales, incluyendo el voto electrónico, y su funcionamiento es muy similar al de la banca electrónica. El objetivo final en Suiza no es remplazar el voto tradicional en papel a través de correo, sino ofrecer un método alternativo, que pueda incrementar la participación ciudadana. En 2009, el cantón de Ginebra fue el primero en aprobar la utilización del voto electrónico por Internet incluyéndolo en su Constitución. En 2011, el cantón de Zurich decidió suspender los ensayos de voto electrónico por razones técnicas y de costos. Sin embargo se piensa en reanudarlos. En la actualidad las pruebas de voto electrónico por Internet o por SMS se realizan en 13 cantones de los 26 cantones que tiene Suiza. La Cancillería Federal coordina los diferentes proyectos cantonales y realiza las autorizaciones necesarias para los ensayos a nivel federal. Las pruebas se centran en suizos residentes en el extranjero.

III.3.- SISTEMAS MIXTOS

III.3.1- E.E.U.U.

Cada Estado e incluso cada Condado deciden autónomamente sobre la forma y recursos electorales a utilizar. En 1892, debutó la primera máquina de votación denominada “Myers Automatic Booth,”, se trataba de un sistema basado en el uso de palancas mecánicas, en el que a cada candidato se le asignaba una palanca. En 1930, estas máquinas fueron instaladas en las principales ciudades de Estados Unidos y en 1960, casi la mitad de la población votaba con estas máquinas.

Desde 1980 han existido cinco tipos de sistemas de votación: máquinas de palanca, tarjetas perforadas, papeletas de votación con o sin sistemas de escaneo óptico y máquinas de grabación electrónica directa o DRE (máquinas que graban los votos por medio de una papeleta de votación en forma de pantalla provista de botones o pantallas de digitalización que pueden ser activados por el votante). En 1996, el 24,6% de los votantes para las elecciones presidenciales utilizaron el sistema Marksense, de escaneo óptico. El 7,7% utilizaron votación electrónica directa DRE.

En las elecciones presidenciales de 2000, tan sólo el 1,6% del electorado usó papeletas convencionales de papel; el 9.1% usó el registro electrónico directo, el 18.6% usó las máquinas de palanca, el 27,3% usó lectores ópticos y el 34.3% usó las tarjetas perforadas. En el estado de Florida, se registraron incidencias con el sistema de votación de tarjetas perforadas en el recuento de votos. Además, doscientos militares destinados fuera del país votaron a través de Internet.

En 2002, el Congreso aprobó la Ley Hava (Help America Vote Act), que ordenaba mejorar las prácticas electorales en todo el país asignando fondos para reemplazar los sistemas de tarjetas perforadas y máquinas de palanca y pasar a sistemas de votación más avanzados. En 2004, en las elecciones presidenciales, el 13,7% de los electores votaron con tarjetas perforadas; el 14% usó máquinas de palancas; el 34,9% equipos de lectura óptica y el 29,3% utilizó votación electrónica directa, DRE.

En 2008, en las elecciones primarias demócratas se permitió a los residentes en el extranjero emitir el voto a

través de Internet. También, en las elecciones generales, el condado de Okaloosa en Florida realizó una prueba piloto vinculante en la que los militares desplazados votaron por Internet.

En 2012, en las elecciones presidenciales el 56% de los votantes utilizaron papeletas de papel con o sin sistema de escaneo óptico y el 39% máquinas de votación electrónica (DRE). En estas elecciones, se produjeron largas colas y algunos problemas técnicos en diferentes Estados. Los soldados de seis Estados desplegados en el extranjero y residentes fuera del país pudieron ejercer el voto por Internet.

III.3.2.- Filipinas

En 2007, se utilizó por primera vez, de forma vinculante, el voto por Internet para los filipinos residentes en el extranjero. En 2008, con el fin de determinar la tecnología a utilizar en las elecciones de 2010, se realizó una prueba piloto mediante dos sistemas de grabación: uno mediante máquinas de votación con pantalla táctil y otro con lector óptico.

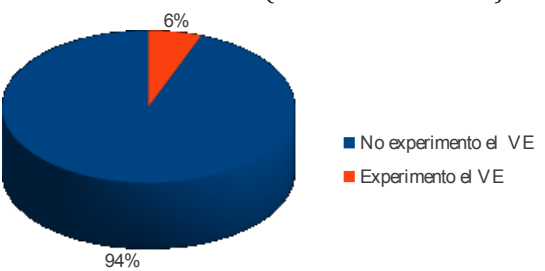
En 2010, se realizaron las elecciones legislativas por primera vez con votación electrónica. Se reconocieron irregularidades por parte de la Comisión Electoral de Filipinas y se creó una Comisión para investigar las denuncias. En 2013, se volvieron a realizar elecciones legislativas con el mismo sistema de voto electrónico que en el 2010 y sin incidencias.

III.4.- CONCLUSIONES SOBRE EL USO DEL VOTO ELECTRÓNICO EN DISTINTOS PAÍSES

Con excepción de Latinoamérica, de los 238 países solo 14 han experimentado el uso del voto electrónico; de ellos solo 2 lo han adoptado, 4 lo han prohibido o paralizado su uso y 8 continúan sus estudios y pruebas.

Se puede apreciar que fuera de Latinomérica el porcentaje de países que han experimentado el voto electrónico es sensiblemente menor (la mitad) que si se considera la totalidad de los países del mundo. Esto se puede ver en el siguiente gráfico:

Gráfico III Países que experimentaron el Voto Electrónico (Sin Latinoamérica)



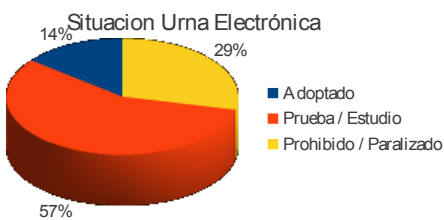
En la mayoría de los casos el sistema de urna electrónica fue desarrollada por el sector privado y solo en uno de ellos se usó un sistema de código abierto, aunque por parte de una empresa privada. Un resumen de esto se expone en la tabla II.

Tabla II Situación de la urna Electrónica (excluido Latinoamérica)

PAÍS	ESTADO V.E	PUB./PRIVADO	COD.
ALEMANIA	PROHIBIDO / PARALIZADO	PRIVADO	NO
AUSTRALIA	PRUEBA / ESTUDIO	PRIVADO	SI
BÉLGICA	ADOPTADO	PRIVADO	NO
ESPAÑA	PRUEBA / ESTUDIO	PRIVADO	NO
EMIRATOS ÁRABES UNIDOS	PRUEBA / ESTUDIO	PRIVADO	NO
FINLANDIA	PROHIBIDO / PARALIZADO	PRIVADO	NO
FRANCIA	PRUEBA / ESTUDIO	PRIVADO	NO
HOLANDA	PROHIBIDO / PARALIZADO	PRIVADO	NO
INDIA	ADOPTADO	PRIVADO	NO
IRLANDA	PROHIBIDO / PARALIZADO	PRIVADO	NO
JAPÓN	PRUEBA / ESTUDIO	PRIVADO	NO
KAZAJISTÁN	PRUEBA / ESTUDIO	PRIVADO	NO
NORUEGA	PRUEBA / ESTUDIO	PRIVADO	NO
RUSIA	PRUEBA / ESTUDIO	PRIVADO	NO

El porcentaje de rechazos a los sistemas de urna electrónica duplica a los de adopción del sistema, aunque el caso de países que continuarán las pruebas y estudios es el doble de los que rechazaron el sistema. Esta situación se pone de manifiesto en el gráfico IV. Debe señalarse también que la mayoría de los rechazos de los sistemas basados en urna electrónica no eran de código abierto o público y fueron realizados por empresas privadas.

Gráfico IV Resultados de uso de la urna electrónica en el mundo (Sin Latinoamérica)



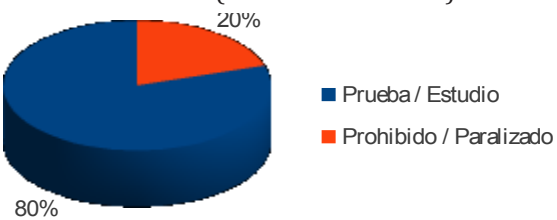
En los países que experimentaron la tecnología celular, no se registraron adopciones del sistema y uno de ellos lo prohibió, como muestra la tabla

Tabla III Situación del voto con tecnología celular (excluido Latinoamérica)

País	Estado V.E	Pub./Privado	Cod. Abierto
Canadá	Prueba / Estudio	Privado	No
Corea del Sur	Prueba / Estudio	Privado	No
Estonia	Prueba / Estudio	Privado	No
Reino Unido	Prohibido / Paralizado	Privado	No
Suiza	Prueba / Estudio	Privado	No

El escaso número de países que experimentaron con el voto mediante tecnología celular no nos permite sacar conclusiones válidas, salvo señalar que la mayoría continúa sus pruebas y estudios, esto posiblemente se deba a que esta tecnología está en constante evolución y presenta continuamente nuevas alternativas. La distribución de los resultados para el voto con tecnología celular se muestra en el siguiente gráfico:

Gráfico V Resultados del voto con tecnología celular en el mundo (Sin Latinoamérica)



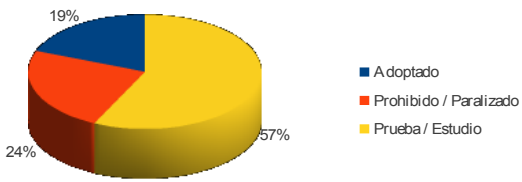
Respecto del uso de la urna electrónica y tecnología celular, solo se registran dos experiencias que resultaron adoptadas, como muestra la tabla IV.

Tabla IV Situación del voto con urna y tecnología celular (excluído Latinoamérica)

PAÍS	ESTADO V.E	PUB./PRIVADO	COD. ABIERTO
E.E.U.U.	SI	PRIVADO	NO
FILIPINAS	SI	PRIVADO	NO

Analizando el total de las experiencias sobre los distintos sistemas de voto electrónico en el mundo (sin Latinoamérica), se aprecia que el 60% continúa realizando pruebas y estudios, y los rechazos superan ligeramente a las adopciones de algún sistema de voto electrónico. Esto se aprecia en el siguiente gráfico.

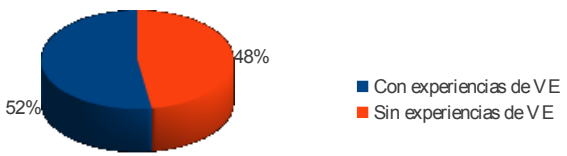
Gráfico VI Resultados del uso de los distintos sistemas de voto electrónico en el mundo (sin Latinoamérica)



IV
EXPERIENCIAS EN AMÉRICA LATINA

En América Latina se produce un hecho interesante, 11 de los 21 países han experimentado el voto electrónico, lo cual representa una notable diferencia con lo que ocurre en el resto del mundo. Esto puede verso en el siguiente gráfico.

Gráfico VII Países que experimentaron el voto electrónico en Latino América



IV.1.- DETALLE DE LAS EXPERIENCIAS EN CADA PAÍS

IV.1.1.- Brasil

Brasil es el único país del continente americano que ha implementado un sistema de voto electrónico en una elección nacional. Para implementar el 100% de este sistema en su territorio, el Tribunal Superior Electoral (TSE) empezó gradualmente a automatizar los diferentes procedimientos que forman parte del sufragio y el escrutinio. El TSE viene implementando un sistema de identificación de los votantes, con lo cual el Brasil pasaría a ser el único país en automatizar todas las fases del proceso electoral. En las elecciones generales del 3 de octubre de 2010, el sistema de votación electrónica

permitió, que luego de casi tres horas de haber concluido el sufragio, se contara con los resultados del 90% de los votos emitidos por más de 135 millones de electores.

Sin embargo, la implementación del voto electrónico ha seguido un largo proceso:

- La primera elección donde se recurrió al uso de la computación fue en las elecciones generales de 1982. En esa oportunidad se permitió el uso de computadores para el recuento de votos en el Estado de Río de Janeiro. A partir de entonces el uso de la informática en los procesos electorales brasileños fue en aumento y abarcando otras áreas.
- En octubre de 1995 se aprobó la Ley Electoral que marcó las directrices del voto electrónico con la intención de eliminar el fraude electoral y reducir el tiempo del escrutinio.
- En el año 1996 fue la primera vez que algunos electores brasileños entraron en contacto con una micro computadora que les permitía elegir a su candidato y registrar su voto.
- En 1997, se organizó en Internet el Forum de Voto Electrónico para discutir el voto electrónico en Brasil. El grupo de electores allí reunido comenzó a publicar artículos técnicos y políticos, a presentar trabajos en congresos científicos, a producir disertaciones de maestrías, y también se iniciaron trabajos de concientización junto a senadores y diputados, incluso con la presentación de un documento público conocido como “Alerta de los Pro-

fesores" que ya cuenta con casi un millar de firmas de apoyo, de juristas de renombre, docentes, especialistas en informática y periodistas.

Por primera vez en tres municipios en las elecciones de 2008, el sistema registró las imágenes de los dedos de las manos del elector, sin embargo y como forma de seguridad, el miembro de la mesa electoral tenía a su disposición una hoja con las fotos de todos los electores para confirmar su participación. De esta forma se hizo prácticamente imposible en Brasil la posibilidad de que una persona votara más de una vez.

El TSE de Brasil es la institución encargada de organizar y administrar todas las elecciones, además de serle otorgado por parte de la Constitución Política el poder de decidir sobre todos los litigios electorales, siendo la última instancia en esta materia. Por otro lado, tiene como función reglamentar las leyes electorales aprobadas por el Congreso Nacional, y su interpretación e implementación forman parte de sus competencias. Todo esto evidencia una concentración de poder en el organismo electoral que reglamenta, organiza, fiscaliza y juzga sus propios actos.

Actualmente, las elecciones brasileñas son una de las más informatizadas del mundo, el 100% de los votos presenciales son emitidos electrónicamente y la tecnología que emplea ha sido exportada a otros países: Paraguay, Argentina, Ecuador, Costa Rica, República Dominicana y México han firmado acuerdos con el TSE, para usar la urna electrónica en pruebas o elecciones vinculantes.

Varias tecnologías han sido desarrolladas en Brasil, entre ellas, se resalta el desarrollo de urnas biométricas que procesaban el voto a partir de la identificación biométrica del elector, con lo cual Brasil se posicionó como el país a la vanguardia tecnológica de los procesos electorales en todo el mundo. Las urnas electrónicas, en términos generales, tuvieron éxito entre los electores, principalmente porque terminaron en un alto porcentaje con una serie de fraudes que eran posibles en el sistema manual. La ausencia de noticias sobre posibles errores y fallas del sistema contribuyó, en gran parte, a la buena aceptación del sistema. Aunque, según Tula (TULA,2005): "Esta ausencia de noticias no se debe a la ausencia de errores y fallas, sino a la falta de transparencia del sistema, que limita mucho el surgimiento de este tipo de información. Por ejemplo, en el estado de California, (EEUU), después de las primarias del partido Demócrata en mazo de 2004, el fabricante de máquinas de votar Diebold fue desacreditado como proveedor después de que se descubrió que los programas de las máquinas habían sido alterados en relación a los homologados, y los responsables intentaron esconder el hecho. El órgano responsable por la fiscalización, la Secretaria de Estado, tuvo cómo detectar el problema, asignar responsabilidades y castigar en menos de dos meses. En las elecciones del 2000 en Brasil, ocurrieron exactamente los mismos problemas: los programas homologados por los fiscales de los partidos políticos fueron modificados posteriormente y, en las urnas del 2000, se utilizó una versión no homologada. Pero esto fue ocultado a los fiscales y electores por los responsables del sistema".

El resultado de la actividad de la sociedad civil organizada, obtuvo una mayor transparencia electoral, ya que, con las presiones sobre el TSE para que diera explicaciones, se obtuvo permiso para la elaboración de tres análisis técnicos por parte de entidades universitarias: El reporte de la Universidade de Campinas, el de la Fundación COPPETEC de la Universidade Federal do Rio de Janeiro y el informe de la Sociedade Brasileira de Computação realizado por profesores de la Universidade Federal de Minas Gerais y de la Universidade Federal de Santa Catarina .

Estos reportes revelan diversos problemas de confiabilidad y fallas en la seguridad del sistema electoral brasilero, y dejan en evidencia que la fiscalización permitida no tiene las condiciones necesarias para detectar problemas graves si ocurrieran.

IV.1.2.- Colombia

El Sistema Electoral Colombiano cuenta con dos instituciones, que intervienen en el desarrollo de los procesos electorales: el Consejo Nacional Electoral (CNE) y la Registraduría Nacional del Estado Civil. El CNE, tiene entre sus funciones ejercer la inspección y vigilancia de la organización electoral, velar por el cumplimiento de las normas sobre partidos políticos, efectuar el escrutinio general de toda la votación nacional, entre otras, Las funciones de la Registraduría Nacional son las de organizar el proceso electoral, llevar el censo electoral y proteger el ejercicio del derecho al sufragio. A partir, de los problemas suscitados en las elecciones de congresales de marzo del 2002, donde hubo denuncias de adulteración de

resultados, manipulación en la designación de jurados y, en general, de intervención indebida en el desarrollo del proceso de las instituciones encargadas de llevarlo adelante, se tomaron iniciativas para fortalecer el sistema y dotarlo de mayor confiabilidad. En primer lugar se impulsó el cambio de cédula de todos los colombianos, una segunda iniciativa fue la implantación del voto electrónico, aprobando la Ley 892 de 2004 sobre el voto electrónico. Desde ese momento, se acepta los tres sistemas de votación electrónica, que existen en el mundo: el voto electrónico por medios informáticos (TIC), las urnas electrónicas con registro en base de datos electoral, y voto electrónico telemático o vía Internet a un portal oficial. El Código Electoral, faculta al gobierno a tecnificar y a sistematizar el proceso electoral especialmente en lo relacionado con la actualización de los censos, expedición de documentos, preparación y desarrollo de las elecciones, utilizando los medios más modernos en esta materia.

A pesar de contar con una legislación, que faculta la implementación del voto electrónico, aún se continúa en una fase de pruebas y experimentación. Actualmente, los padrones, el sufragio y el conteo de votos se realizan en forma manual. Desde el año 2009, se hacen pruebas para su automatización en elecciones a nivel departamental y municipal con algunos dispositivos tecnológicos de plena identidad del elector. El documento de identidad, provisto por la Registraduría Nacional a todos los ciudadanos colombianos mayores de 18 años, es el documento útil para sufragar, y automatiza la información del padrón: nombre, foto, huella dactilar y la firma.

En las elecciones presidenciales y congresales de 2006, se realizaron pruebas con dos sistemas diferentes: la primera utilizó tarjetas, habilitadas por los jurados, que permitían al ciudadano votar por el partido y candidato de su preferencia; en la segunda, el ciudadano podía ver todas las opciones en una tarjeta electoral preimpresa y podía emitir su voto a través de una pantalla táctil. Para facilitar el ejercicio del sufragio los electores fueron capacitados antes de entrar a los locales de votación, pudiendo hacer ensayos antes de votar efectivamente. Al mismo tiempo se proyectaron videos de capacitación fuera de los locales. A pesar, de haber realizado pilotos con voto electrónico, el sistema electoral colombiano no cuenta con una solución tecnológica propia, sino que ha sido proporcionado por empresas privadas.

Colombia concluyó, que la implementación del voto electrónico debe hacerse de forma progresiva, ya que no hay obligación de establecerlo en un 100%, debido a, que ante el conflicto interno, se puede considerar la posibilidad de dejar en las zonas de alto riesgo el método manual. Los dos los problemas que se pretende solucionar con la implementación del voto electrónico son:

- Acabar con la suplantación de las personas al votar y depurar las bases del censo electoral.
- Evitar la manipulación fraudulenta de los resultados electorales.

Para lograr lo anterior se debería adoptar un sistema de voto con las siguientes características:

- Máquinas de recepción y almacenamiento de la infor-

mación electoral que disminuya la presencia y participación humana en el manejo de los resultados.

- Totalizadores electrónicos de la votación.
- Aparatos de lectura biométrica que permitan constatar, que la persona que se presenta a la votación, corresponde a la identificación del documento presentado y, que está incluida en la base de datos de personas habilitadas para votar.

Por otro lado, en zonas alejadas del país se encuentran dificultades, como ser:

- Problemas con las fuentes de energía para las máquinas.

La falta de comunicación vía Internet, lo que debilita el sistema.

Por ello, se solicitó a las registradurías de los municipios mantener un plan de emergencia, para contar con los generadores de energía necesarios para soportar el proceso y el conteo de los votos en caso de manipulación de las plantas de energía principales. Sin embargo, desde la MOE se cree que se ha planteado mal el debate, dado que el voto electrónico es una herramienta que no va a solucionar problemas que se tienen frente a anomalías, irregularidades y delitos electorales. Es decir, en palabras de Alejandra Barrios (funcionaria del MOE): "A través del voto electrónico tu no solucionas trashumancia electoral, a través del voto electrónico, tu no solucionas el problema de compra o venta de votos, a través del voto electrónico tu no solucionas la utilización de subsidios del Estado o programas para favorecer determinados candidatos. ¿Qué se puede solucionar? la rapidez en el conteo de los

votos, mayor confiabilidad en el conteo de los votos dependiendo del sistema que se está utilizando".

También, se debe garantizar que los partidos políticos cuenten con auditores expertos en sistemas, porque los miembros de los partidos deben ser los primeros en señalar que confían en el sistema, dado que a través de esto se puede velar por la eficacia, la eficiencia y la veracidad en el conteo de los votos. Por último, la MOE hizo algunas recomendaciones refiriéndose a las pruebas en las elecciones internas de los partidos, programada para finales del 2012, señalando que el voto electrónico es un cambio de cultura del voto, donde debe producirse una familiarización de la ciudadanía con los elementos tecnológicos. Para ello, se han realizado pequeñas pruebas piloto a lo largo del país, donde se evaluó si el sistema permite votar más de una vez, si permite modificar el voto, si los jurados pueden corroborar los resultados emitidos, si la identificación del votante está relacionada con el voto realizado, y si el funcionamiento de las máquinas es adecuado. Así mismo, se analizaron aspectos informáticos, como ventajas y desventajas de las maquinas, del proceso de votación, experiencia electoral de las empresas, riesgos que pueden tener y posibilidad de solucionar problemas como fallas en la máquina o cortes eléctricos, entre otros.

- También, se aprobó invitar a organismos multilaterales y agencias de cooperación internacional con experiencia en procesos de voto electrónico para que acompañen en la definición del modelo de voto electrónico a adoptar. Sin embargo aún está pendiente analizar temas como:

- Modelos de voto electrónico, con base en los resultados de las encuestas aplicadas a los proveedores, las tecnologías.
- Un documento de trabajo con los requisitos, que de acuerdo con el órgano de control, debería reunir el sistema.

Definición de los requisitos mínimos que debe reunir el voto electrónico.

En Colombia hay personal suficientemente capacitado para desarrollar su propio proceso de voto electrónico, sin embargo, las dificultades que se puedan presentar son de naturaleza política y no tecnológica.

IV.1.3.- Costa Rica

En 2002, se realizó una prueba con dispositivos de registro electrónico directo y comprobantes Durante esas elecciones, el elector podía elegir emitir el voto a través del método tradicional de papel, o a través de la urna electrónica diseñada por el Tribunal Supremo Electoral (TSE). Cuando el elector elegía votar por el medio electrónico, se le entregaba un comprobante en blanco debidamente firmado al dorso por los miembros de mesa presentes, en el cual se imprime la voluntad del votante. Posteriormente accede a la máquina de votación electrónica y realiza en la pantalla su elección, la cual es impresa en el comprobante. Finalmente el votante dobla el comprobante de tal manera que estén visibles las firmas de los funcionarios de casilla, y es depositado en una urna. En esta prueba se eligieron 133 juntas, lo cual se tradujo en más de 80.000 votos reales con valor vinculante que

fueron emitidos electrónicamente. Estas cifras representan únicamente un 6% del electorado, lo cual permite suponer que serán necesarias un gran número de mejoras al proceso para poder ser usados en futuras elecciones.

IV.1.4.- Ecuador

En 2004, en las elecciones seccionales se utilizaron las urnas brasileñas y los resultados fueron vinculantes. En 2013 la Comisión Electoral de la Federación de Rusia y el Consejo Nacional Electoral de Ecuador firmaron un acuerdo para recibir asesoramiento para la implantación del voto electrónico. También, se firmó un convenio de cooperación para el voto electrónico Azuay de 2014, entre la Dirección Nacional Electoral de Argentina (DINE) y el Consejo Nacional Electoral de Ecuador. En virtud de estos convenios, en las elecciones locales de 2013 se utilizaron, en 3 provincias, 3 tecnologías distintas de voto electrónico: voto electrónico con comprobante impreso del voto, boleta con chip electrónico y registro electrónico del voto. El 10% del censo electoral utilizó alguno de estos sistemas.

IV.1.5.- Guatemala

En 2002, para las elecciones de alcaldes y síndicos se utilizó votación electrónica: en la pantalla se presentaban los candidatos y en un teclado numérico el elector decidía.

IV.1.6.- México

En 2005, se realizaron pruebas piloto en el estado de Coahuilla en las elecciones para Gobernador, diputados

y alcaldes. Este estado es el más avanzado en materia de voto electrónico. Después de algunas pruebas piloto, en las elecciones del estado de 2008, se utilizaron 100 urnas electrónicas, con pantalla táctil y la votación tuvo carácter vinculante. También ha habido experiencias de voto electrónico en Distrito Federal y Jalisco.

En cuanto al voto por Internet, el Instituto Federal Electoral (IFE) lo implementó para los mexicanos residentes en el extranjero en las elecciones presidenciales de 2012. La experiencia no tuvo buenos resultados, en particular por el alto costo.

IV.1.7.- Panamá

En 2014, las elecciones presidenciales convocaron a 4.859 electores, de los 2,4 millones, que votaron electrónicamente en un colegio de la ciudad de Panamá. El sistema utilizado fue mediante máquinas con pantalla táctil. El Tribunal Electoral calificó la experiencia de éxito, pero indicó, que se deben tomar medidas para optimizar el sistema.

IV.1.8.- Paraguay

Se realizó, una primera experiencia exitosa, en el año 2001, y dos experiencias adicionales en elecciones presidenciales y municipales, que lo encaminaron a automatizar el voto en todas las mesas electorales, sin embargo, las dudas planteadas por candidatos derrotados en elecciones internas de algunos partidos políticos, donde se utilizó el sistema de voto electrónico, generó un manto de duda, por lo cual, el gobierno decidió regresar al sistema manual tradicional en las elecciones presidenciales del 2008.

La automatización de los procedimientos electorales en Paraguay ha sido desigual. La primera experiencia de voto electrónico en Paraguay se dio con las elecciones municipales del año 2001, en el marco del "Plan Piloto Urna Electrónica". Su implementación fue dispuesta por el Tribunal Superior de Justicia y contó con el apoyo del Tribunal Superior Electoral del Brasil, quien facilitó las urnas electrónicas y brindaron asistencia técnica y política. También, se recibió la asesoría de la OEA y un aporte financiero del gobierno de los EEUU. La elección se llevó a cabo en siete municipios, con 34.098 electores (un 1,56% del padrón electoral). Uno de los rasgos sobresalientes de esta experiencia es que el voto electrónico logró incrementar la participación electoral media histórica allí donde fue aplicado.

Una segunda prueba, mucho más ambiciosa se realizó para las elecciones presidenciales del 2003. En esa oportunidad el 53% del electorado paraguayo, en 33 distritos electorales, emitió su voto a través de una urna electrónica brasilera. De la totalidad de los distritos, 11 dispusieron urnas en la totalidad de las mesas y 22 lo hicieron de forma parcial. Como forma de evitar las dudas y mejorar la confianza en el sistema, TSJE hizo que participaran todos los partidos políticos en el proceso de preparación y ejecución del proyecto: la carga de las urnas, los controles informáticos y todas las operaciones necesarias, que pudiesen otorgar mayor transparencia y confianza al proceso. Así, los partidos actuaron en calidad de cogestores, acompañando la propuesta general de introducir nuevas tecnologías al proceso electoral.

Para las elecciones municipales del 2006, el TSJE resolvió implementar el sistema mixto de votación en colaboración con el TSE de Brasil.. En 21 distritos se utilizaron, únicamente urnas electrónicas, mientras que en 7 la elección fue sólo por el método tradicional; en los restantes distritos se utilizaron ambos métodos en un 50% cada uno. También, se utilizó voto electrónico en las elecciones internas de los partidos políticos. Esto fue establecido por la ley 2851 de 2005, que impuso la obligatoriedad del uso de las urnas electrónicas y así se hizo en 8 internas partidarias. Sin embargo, en las últimas elecciones generales, en el año 2008, se volvió al sistema tradicional, dejando de lado las urnas electrónicas, dado que, en las elecciones internas de los partidos políticos paraguayos se generó disenso, dado, que algunos candidatos derrotados en las elecciones internas, denunciaron fraude en el sistema de votación electrónica. Ello creó desconfianza en el sistema y motivó que los partidos políticos solicitaran volver al sistema manual de votación.

Según la Misión de Observación Electoral de la OEA, que estuvo presente en las elecciones de 2008, el sistema jurídico paraguayo está dentro del estándar aceptable, el problema no radica en la legislación misma sino en su falta de aplicación. A ello hay que agregar la falta de confianza de los actores políticos entre sí, que los lleva a pensar en la posible manipulación de las urnas electrónicas por parte de sus adversarios.

IV.1.9.- Perú

Desde 1990, se han realizado diversas experiencias de voto electrónico presencial y no presencial en distintos procesos electorales, como ser: elecciones internas en organizaciones políticas, comités distritales en municipalidades, municipios escolares, colegios profesionales, organizaciones de la sociedad civil y en consultas populares.

La aprobación de la Ley 28581 de julio de 2005, en su primera disposición complementaria, autorizó la implementación progresiva y gradual del voto electrónico en Perú, la cual debía garantizar la seguridad y confidencialidad de la votación, la identificación del elector, la integridad de los resultados y la transparencia en el proceso electoral. Posteriormente, en octubre de 2010, el Congreso de la República aprobó la Ley 29603 de 2010, la cual autorizó a la Oficina Nacional de Procesos Electorales ONPE emitir las normas reglamentarias para la implementación del voto electrónico. Así, la ONPE, junto al Jurado Nacional de Elecciones (JNE), que administra la justicia electoral, y el Registro Nacional de Identificación y Estado Civil (RENIEC), que confecciona el padrón de electores, constituyen en su conjunto el Sistema Electoral Peruano. La ONPE se convirtió en el organismo especializado en organizar y ejecutar los procesos electorales en el Perú, desarrollando una solución tecnológica de voto electrónico de acuerdo a requerimientos propios y diversas evaluaciones sobre aspectos legales, organizacionales, tecnológicos y socioculturales. Dicha solución tecnológica consta de dos modalidades: el voto electrónico presencial (VEP) y el voto electrónico no presencial

(VENP). Los primeros ensayos de votación electrónica se realizaron en el año 1996, en dicha oportunidad se adquirieron 70 máquinas de votación de la empresa IBM, similares a las utilizadas en las Elecciones Municipales en Brasil, el mismo año.

Las demostraciones continuaron en las Elecciones Regionales y Municipales de 2002, donde se colocaron máquinas de votación electrónica en un centro comercial, y se contó con la visita de 1700 electores diarios en una jornada de 15 días. Las máquinas de votación empleadas eran una primera solución tecnológica preparada por la ONPE. En esa oportunidad, se utilizaron pantallas sensibles al tacto que mostraban al elector las opciones de sufragio en la cédula de votación electrónica. Dicho sistema se complementaba con una Estación de Administración, que utilizaba el presidente de mesa para comprobar la identidad del elector y asignar las cabinas de votación correspondientes.

Por otro lado, se debe señalar, que la adopción del voto electrónico se ha perfilado como una posible solución a los problemas registrados con el método tradicional de elección, sin embargo, diversas pruebas piloto, en especial la del 2006, produjo resultados desfavorables, dado que, ninguna empresa presentó un programa confiable y seguro para el proceso de votación electrónica. Se generaron una serie de críticas a la labor de la oficina de procesos electorales ONPE, por la lentitud en el conteo oficial de los votos, lo cual llevó a que en el 2010, el Congreso peruano aprobara el reglamento que permite poner en vigencia el voto electrónico, para las elecciones del 2011.

Sin embargo, se ha criticado el proceder del gobierno al no tomar las precauciones necesarias de capacitar a la población, siendo lo primero que debe hacer, dado que, un porcentaje considerable de la población aún se encuentra en un analfabetismo digital y no está preparada para comprender un nuevo método de votación.

Ante ello, y tomando como ejemplo el éxito de Brasil en la adopción del voto electrónico, se hará necesario establecer una adecuada estructura tecnológica, siempre y cuando la población peruana esté preparada para adoptar este tipo de mecanismo tecnológicos de elección. Pues, pese a existir voluntad para implementar el voto electrónico en algunas regiones del mundo, se debe evaluar las condiciones de igualdad regional y los costos económicos, sociales y políticos que conllevará la introducción del voto electrónico en un país determinado. De ahí, que la investigación busque evaluar el caso peruano, dados los índices de desigualdad en términos de acceso a Tecnologías de la Información y la Comunicación (TIC´s) y las condiciones económicas y sociales que imposibilitan la implementación del voto electrónico a nivel nacional.

En el marco de la modernización de los procesos electorales en América Latina y en atención al perfeccionamiento continuo de los procesos electorales, han surgido rutas y opciones relacionadas con los avances informáticos, ya que los procesos de incorporación de Tecnologías de Información y Comunicación tienen frente a si una serie de barreras que retrasan muchos de los procesos que permiten el desarrollo de una población, dichas barreras pueden agruparse en cuatro clases y deben ser resuel-

tas o por lo menos reducidas para mejorar la capacidad o preparación de un país. Estas barreras son:

- Infraestructura de formación.
- Ingreso.
- Educación y capacitación.
- Normas y regulaciones al mercado.

El problema de infraestructura es crítico para Perú, ya que los niveles de cobertura de telefonía e Internet son bastante deficitarios y cuentan con redes de bajas prestaciones. Lima y los centros urbanos del interior concentran la mayor oferta de servicios de telecomunicaciones, esto se debe al reducido tamaño del mercado, la dispersión de la población, y las dificultades geográficas y materiales para prestar el servicio. Además, se debe señalar, que en los hogares rurales del Perú el 71% carece de electricidad, y más del 98% de servicios de telecomunicación, mientras, que en los hogares urbanos el 51% carece de servicio eléctrico y el 62.9% no tiene ningún servicio de telecomunicación en casa.

Sin embargo, la mayor dificultad para que Perú tecnifique sus procesos de votación se debe a los limites políticos, que se han generado a partir de los órganos de representación electoral y por los procesos o debates que se han dado dentro del órgano legislativo, que en cierta forma han limitado la reglamentación de la Ley 28581 de julio de 2005, la cual modifica la ley orgánica de elecciones. En 2011, se realizó la primera experiencia vinculante con voto electrónico presencial en el distrito de Pacarán, en las elecciones presidenciales.

En el año 2012, se utilizó de nuevamente y en las elecciones municipales y regionales de octubre de 2014, se utilizó el voto electrónico en siete distritos (34.672 electores y 186 mesas). Se registraron fallos por la falta de capacitación de los técnicos, miembros de mesa y electores, lo cual originó retraso en el proceso de votación. Los resultados se conocieron siete horas después del cierre ya que hubo partidos que solicitaron el cotejo de los votos.

IV.1.10.- Venezuela

En agosto de 2004, el gobierno realizó un referéndum a nivel nacional utilizando tecnología de voto electrónico, con observadores internacionales y miembros de la Organización de los Estados Americanos. El sistema electrónico de voto utilizado en esta consulta fue desarrollado por un consorcio americano-venezolano, que permitió votar por medio de un sistema de pantalla táctil, y cada voto respaldarlo con un registro en papel. La empresa ha realizado esfuerzos por implementar sistemas de votación electrónica que pretenden dar validez a sistemas electorales que se han visto minados por alegatos de fraude y manipulación de votos. Estas fuentes de controversia han incluido la capacidad bidireccional de las máquinas, ya que la información podía fluir desde las máquinas hacia los centros de tabulación, así como de los centros de tabulación hacia las máquinas, las listas electrónicas de votación, pues se temía que las listas fuesen a ser modificadas de tal manera que se beneficiara a algún partido, y el uso de máquinas de identificación por huella dactilar ligadas a las listas electrónicas de votación. Si tomamos en cuenta la importancia de este ejercicio electoral vinculante, su gran representati-

vidad, la fuerte misión de observadores internacionales, y el nivel de publicidad internacional que recibió, este es un buen ejemplo de cómo el voto electrónico demuestra ser un elemento seguro y confiable que, acompañado con un registro de papel que permita auditar los resultados emitidos, ha permitido a muchos países recuperar su democracia y participación ciudadana en los procesos electorales.

En 2006, el Consejo Nacional Electoral introdujo nuevamente la emisión de sufragios a través de urnas con pantallas sensibles al tacto en la elección presidencial de diciembre de 2006. En esta elección, entre los observadores electorales internacionales hubo algunos de gran relevancia como la Agencia de Noticias para la Difusión de la Ciencia y la Tecnología de Castilla y León en España, la que calificó este proceso como exitoso, aunque señaló dificultades con el software al momento de contabilizar los votos, así como errores humanos durante la votación, o la Misión de Observación Electoral de la Unión Europea, quienes congratularon al Consejo Nacional Electoral, así como sus actores políticos y movimientos sociales, por crear condiciones para llevar a cabo elecciones, que son aceptables para todos los participantes. No obstante, este país ha ido realizando mejoras a su sistema y pretende extender el uso de estas tecnologías para futuros procesos. Para estas elecciones, la Comisión Nacional Electoral introdujo diversos métodos de auditoría para garantizar la transparencia y precisión del conteo de los votos: primero, se auditó extensivamente el software bajo el cual funcionaban las máquinas y el hardware mismo de estas, se introdujo un sistema de hot audit, o auditoría calien-

te, llevada a cabo la noche misma de las elecciones, y un sistema de auditoría sobre el rastro de papel que las máquinas dejaban por cada voto emitido.

Otro ejemplo extraído de la experiencia de este país incluye el ejercicio repetido que llevaron a cabo entre diciembre de 2007 y febrero de 2009 para, a manera de referéndum, consultar a la población sobre la eliminación de los límites al periodo presidencial, entre otros temas. El sistema utilizado en este ejercicio fue el mismo que se utilizó en 2004, y desde entonces ha servido para tres referéndums nacionales, una elección presidencial, y una elección parlamentaria; además de ser utilizado en elecciones regionales y municipales.

IV.2.- CONCLUSIONES SOBRE LAS EXPERIENCIAS DE LATINOAMÉRICA

Latinoamérica es una de las regiones con mayor porcentaje de países que han experimentado el voto electrónico, de entre ellos Brasil y Venezuela lo han adoptado y solo un país, Paraguay, lo ha prohibido. En todos los casos analizados las experiencias realizadas han utilizado la tecnología de urna electrónica, se ha desarrollado sobre código no público y con la participación de empresas privadas. La historia de los procesos en los distintos países nos muestra que a pesar de mostrar buenos resultados no hay una aceptación plena de esta tecnología por parte de todos los sectores de la vida política; y en todos los casos, incluso en los países que lo han adoptado, hay dudas respecto de las posibilidades de fraude que pudieran ocurrir con esos sistemas.

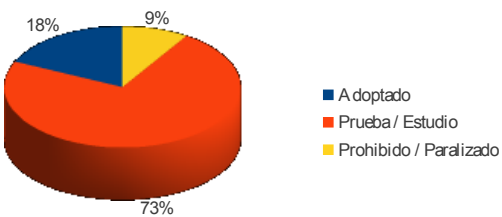
Un resumen de los resultados de las experiencias se muestra en la siguiente tabla:

Tabla V Resultado de las experiencia de voto electrónico en Latinoamérica

PAIS	RESULTADO	PUB/PRIV	Soft Publico	TECNOLOGIA
ARGENTINA	PRUEBA / ESTUDIO	PRIVADO	NO	URNA ELECTRÓNICA
BRASIL	ADOPTADO	PRIVADO	NO	URNA ELECTRÓNICA
COLOMBIA	PRUEBA / ESTUDIO	PRIVADO	NO	URNA ELECTRÓNICA
COSTA RICA	PRUEBA / ESTUDIO	MIXTO	NO	URNA ELECTRÓNICA
ECUADOR	PRUEBA / ESTUDIO	PRIVADO	NO	URNA ELECTRÓNICA
GUATEMALA	PRUEBA / ESTUDIO	PRIVADO	NO	URNA ELECTRÓNICA
MÉXICO	PRUEBA / ESTUDIO	PRIVADO	NO	URNA ELECTRÓNICA
PANAMÁ	PRUEBA / ESTUDIO	PRIVADO	NO	URNA ELECTRÓNICA
PARAGUAY	PROHIBIDO / PARALIZADO	PRIVADO	NO	URNA ELECTRÓNICA
PERÚ	PRUEBA / ESTUDIO	PRIVADO	NO	URNA ELECTRÓNICA
VENEZUELA	ADOPTADO	PRIVADO	NO	URNA ELECTRÓNICA

Del total de experiencias, casi las tres cuartas partes continúa realizando pruebas y estudios, cerda de la quinta parte lo ha adoptado y solo un país lo rechaza. Esto puede verse en el siguiente gráfico;

Gráfico VIII Resultados de las experiencias de voto electrónico en Latino América



V
EXPERIENCIAS EN ARGENTINA

En Argentina se han realizado varias pruebas de votación electrónica a lo largo de la última década. Siendo una república federal cada provincia cuenta con su propia legislación electoral, por lo que existe un grado dispar en el avance hacia la automatización de los procesos electorales. La provincia de Buenos Aires fue una de las primeras en realizar cambios en su legislación e introducir en su normatividad la implementación del voto electrónico. Varias provincias argentinas han legislado su uso, como por ejemplo en Tierra de Fuego y Mendoza que se han realizado elecciones utilizándolo. Todas estas experiencias han sido exitosas y han recibido la aprobación de los electores que han participado en las mismas, lo que hace suponer, que en el mediano plazo, la votación electrónica será aplicada en otras provincias argentinas.

En el año 1988, comenzó la automatización del padrón electoral, este fue un proceso gradual, donde los distritos electorales utilizaron diferente software e incluso algunos distritos siguieron utilizando procedimientos manuales. En el 2003, se siguió avanzando hacia la informatización del Registro de Electores a nivel nacional, pero ya contando con un sistema propio unificado e interconectado dentro de la red del Poder Judicial de la Nación, la reforma de 2009, estableció otros aspectos del proceso electoral, no avanzó sobre el sistema de boleta única y voto electrónico. Si bien, el voto se sigue haciendo

en forma manual, algunas provincias han legislado sobre el voto electrónico y se han realizado varias experiencias (por ejemplo, la provincia de Salta y la Ciudad Autónoma de Buenos Aires). De parte del gobierno federal aún no se ha dado una ley nacional que habilite este sistema para las elecciones generales.

Algunas experiencias que deben citarse son:

V.1.- Provincia de Buenos Aires

Buenos Aires sancionó en el 2003 la Ley 13.082 que modificó la Ley Electoral provincial incorporando un capítulo que faculta al Poder Ejecutivo la implementación total o parcial de sistemas de voto electrónico en los distritos que considere pertinente. Esta ley establece cuales son los requisitos mínimos que deberán tomarse en cuenta, estos son:

- Accesibilidad para el votante: que sea de operación simple para no confundir y no contenga elementos que puedan inducir el voto.
- Confiabilidad: que sea imposible alterar el resultado cambiando votos, contabilizando votos no válidos o no registrando votos válidos.
- Privacidad: que no sea posible identificar al emisor del voto.
- Seguridad: que no sean posibles ataques externos, que esté protegido contra caídas o fallos del software o el hardware o falta de energía eléctrica, que no pueda ser manipulado por el administrador.
- Relación adecuada entre costo y prestación.
- Eficiencia comprobada.

- Dicha ley fue reglamentada en el 2003, donde Buenos Aires optó por las máquinas denominadas Direct Recording Electronic Voting System (DRE). Para su implementación firmó un convenio con el Gobierno Federal de Brasil, quien aportó su know-how y sus urnas, para poder realizar la experiencia piloto, en las elecciones de setiembre de 2003.

La Ley 13.082, que permitió la adopción del voto electrónico en las elecciones generales para la renovación de autoridades del ejecutivo y legislativo fue aprobada en setiembre de 2003, y tuvo vigencia en los comicios de 2005, 2007 y 2009, aunque no se utilizó la modalidad de voto electrónico. Fue en las elecciones realizadas el 28 de marzo de 2010 en Pinamar, para la elección de intendente, donde se utilizó por primera vez la modalidad de voto electrónico para una elección, ya que en las experiencias previas el voto electrónico sólo se había utilizado en las mesas de ciudadanos extranjeros.

V.2.- Ciudad de Posadas. Misiones

En la Ciudad de Posadas, Provincia de Misiones, a partir de la sanción de la Ley XI-N°6, art. 180 y 181, faculta al Tribunal Electoral de la Provincia de Misiones (TEPM) a la implementación, gradual y progresiva, de un sistema de emisión de sufragio y escrutinio por medios electrónicos. El TEPM, a través de sus profesionales y técnicos creó el Voto Codificado Misiones (Vo.Co.Mi.), sistema de votación electrónico, que utiliza una combinación de componentes de hardware y software que permiten al elector imprimir su boleta codificada con un código QR.

La selección de las opciones de votación se realiza sobre una pantalla táctil. Al finalizar la selección se imprime el voto utilizando una impresora térmica sobre un papel tipo rollo térmico. El elector tiene la posibilidad de corroborar que su elección se encuentra debidamente codificada utilizando el lector de código QR, que muestra en pantalla la información contenida en dicho código.

Características del sistema:

- Alcance: disponibilidad del equipamiento.
- Confiabilidad: funcionamiento continuo.
- Auditoría: comprobante en papel.
- Seguridad: secreto del voto.
- Accesibilidad: voto asistido.
- Sencillez y celeridad en el escrutinio.
- No comercial (software libre)

El Vo.Co.Mi., tuvo su debut en las Elecciones Legislativas del año 2013 (5 mesas en centro de votación en Posadas), con gran aceptación por parte de los electores. Luego, se remitió a la Cámara de Representantes de la Provincia de Misiones el informe sobre la implementación del mismo en dichas elecciones. Inscripción del sistema en el Instituto Nacional de Propiedad Industrial (INPI). Expediente N° 20130103860 – Trámite N° 13186243.

En 2015, se utilizó para electores extranjeros (una de cada dos mesas con Vo.Co.Mi.).

V.3.- Otras experiencias

¨La ciudad cordobesa de Marcos Juárez, con unos 16.000 electores utilizaron por primera vez en 2015 la boleta única electrónica. Eligieron intendente y conce-

jales. La experiencia fue todo un éxito. El sistema tecnificado de votación, con su pantalla táctil de por medio, no sorprende mucho a una población que en los últimos años supo tecnificar el proceso productivo ligado a la agricultura. Se trata de máquinas que sólo imprimen boletas electrónicas. Se puede votar por candidato, lista completa o en blanco¨ (conforme Noticias Electorales, 8 de septiembre de 2014)

La única provincia, que aplica para todo el electorado el voto electrónico, es Salta desde 2013 y la Ciudad Autónoma de Buenos Aires desde el 2015, mientras que para las elecciones para Gobernador en Córdoba y Santa Fe, también se utilizaron boletas únicas pero no electrónicas sino de papel.

Las otras provincias donde se ha legislado el uso del voto electrónico son Santiago del Estero, Chaco, Tucumán, Salta, Río Negro, La Rioja y San Luis. Las constituciones de Córdoba y Santa Fé, sólo han permitido la utilización de medios electrónicos de votación para casos de prueba y ensayos.

En la Provincia de Tierra del Fuego también se ha implementado el voto electrónico. Así, en Ushuaia, su capital, se empleó en la elección de intendente y concejales en el año 2003.

Se debe señalar que según la Constitución de 1853, Argentina adoptó la forma de República Federal de Gobierno y divide su territorio en 23 provincias. Siendo Argentina una República Federal donde cada provincia tiene una constitución, la ley es clara en el respeto que

debe salvaguardar cada provincia a los lineamientos establecidos en la Constitución Nacional. Al contar cada provincia con su propia Constitución, con un ente organizador de las elecciones y un juzgado electoral, cada una de ellas tiene la facultad de introducir modificaciones a los procedimientos electorales mientras no contradigan la legislación federal. Esto da como resultado un panorama heterogéneo respecto a los avances de la implementación del voto electrónico.

En Argentina se encuentra vigente el "sistema francés" para elecciones nacionales y en casi todas las provincias, para cargos provinciales y municipales. En dicho sistema, se utiliza una boleta papel por partido político o alianza, con varios tramos según las categorías a elegir. La Junta Nacional Electoral es la encargada de aprobar las boletas electorales conforme el Código Electoral Nacional, pero los partidos políticos son los encargados de la impresión de las boletas. Esto les otorga, la facultad de distribuir las boletas el día de la elección e incluso distribuirlas en los días previos a los comicios. Este sistema ha generado una serie de prácticas fraudulentas, tales como la sustracción de boletas del cuarto oscuro, falsificación de boletas, clientelismo político, el denominado ¨voto en cadena¨, y variadas irregularidades al momento del escrutinio.

Por todo esto, se ha generado una gran desconfianza sobre el proceso electoral, el sistema de votación y respecto a las autoridades electorales que se encuentran a cargo. Como consecuencia ha surgido un reclamo generalizado de la ciudadanía por transparencia, honestidad y eficiencia en la gestión pública, y fundamentalmente,

por comicios limpios que reflejen la verdadera voluntad popular.

Por ello, es importante que se incluya en la agenda política la discusión en torno a una reforma electoral que brinde transparencia al proceso eleccionario. Que se generen cambios para mejorar la calidad de la política, reducir sus costos y efectuar un eficiente control electoral.

Finalmente, se puede concluir que el voto electrónico debe ser considerado como una herramienta y no como la solución a los problemas de la democracia. Puede contribuir a mejorar la calidad de la democracia pero depende de cada sociedad y de una implementación responsable.

El cambio del sistema tradicional de votación por el de voto electrónico debe ser el resultado del consenso de todos los actores políticos y sociales.

El sistema de voto electrónico se consolida dentro de un contexto político fortalecido por instituciones eficientes y transparentes, un sistema de partidos políticos sólido y una gran participación ciudadana.

VI
PROPUESTA DE USO DE LA TECNOLOGÍA EN UNA ELECCIÓN

Ante la demanda de una nueva forma de efectuar el acto eleccionario, se generan varias propuestas y críticas a su respecto. Las propuestas se basan fundamentalmente en alternativas para brindar soluciones a los problemas que se han presentado en la historia de los distintos actos electorales. Una síntesis de estos problemas, podría ser:

- El sistema de boletas partidarias impresas por los partidos políticos genera una gran desigualdad entre los partidos con grandes recursos económicos y los partidos con pocos recursos económicos. Esto se pone de manifiesto, cuando se roban boletas de los partidos en los cuartos de votación y los partidos pequeños carecen de recursos (fiscales y mas boletas para reponer) para afrontar los problemas que surgen en la elección.
- La complejidad de boletas sábanas con alianzas entre fuerzas nacionales, provinciales y municipales, conspira para que elegir una opción independiente que no se integre en una lista sábana, sea algo sencillo.

El sistema de recuento de los votos emitidos en las distintas categorías, se hace en forma manual, sin un procedimiento establecido y regulado; esto genera demoras, interferencias y equívocos accidentales o intencionados.

Como todo sistema pensado para que se actúe sin malicia, el actual sistema fue vulnerado por actos maliciosos, que buscaron beneficio propio o de un sector, o solo entorpecer u obstruir en acto comicial.

Los sistemas de contralor, no actúan en forma independiente de los partidos o intereses en pugna durante la elección. Además, hoy no es posible auditar todos y cada uno de los pasos que integran el proceso, desde su inicio hasta su finalización. Esta capacidad de auditoría está limitada a determinados aspectos de la elección y a determinadas personas, impidiendo el acceso a organizaciones de la sociedad civil.

Existe en el actual sistema, un proceso de digitalización, transmisión de datos y carga provisional de datos, que se realiza en forma electrónica, mediante software propietario con una capacidad de auditoría restringida, ya que los equipos y programas de digitalización de actas de escrutinio, de transmisión electrónica de dichas imágenes digitalizadas y el proceso de carga de las actas, se fiscalizan por observación y simulacros previos, pero sin intervención directa de los fiscales.

- Podrían agregarse varios aspectos que amplíen y completen esta somera descripción de los problemas existentes en el actual sistema electoral. Del mismo modo se presentan varias propuestas que pueden agruparse en distintas categorías, las cuales pueden resumirse en:
- Propuestas de naturaleza política, como ser las restricciones a alianzas múltiples entre distintas categorías electorales (las llamadas “colectoras”).

- Propuestas de naturaleza metodológica, como es el sistema de boleta única.
- Propuestas de naturaleza logística, como generación de recursos monetarios y publicitarios,

Propuestas de naturaleza tecnológica, como sería el voto electrónico.

- Es en esta última categoría, que nos centramos para analizarla y ver qué posibilidades existen para dar respuesta, desde la tecnología, a los problemas que se plantean en el actual sistema electoral. Dado, que muchos partidos políticos proponen el voto electrónico, algo que desde el punto de vista tecnológico es viable y de posible implementación, se deberían revisar las principales críticas que se le realizan a este sistema. Algunos problemas que se plantean, en particular algunos señalados por Busaniche (BARGACH, 2015). no son tales, y puede argumentarse lo siguiente:
- Dificulta la participación ciudadana: este argumento supone que la mayoría de la ciudadanía no puede operar un equipo informático, sin embargo todos los trabajadores reciben su sueldo por medio de un depósito en una cuenta bancaria, que se maneja por medio de terminales computarizados o de home banking, lo mismo ocurre con los jubilados o beneficiarios de planes sociales. Quedaría algún sector de la población, que por razones de edad o de carencias de instrucción tengan dificultades en la emisión del voto, en cuyo caso se podría permitir que estos accedan con algún familiar que los ayude

o que en las cabinas de voto haya algún asistente (auxiliar de las autoridades electorales) que colabore en la emisión del voto. De todos modos un nuevo sistema electoral requiere difusión y capacitación ciudadana, algo que debe hacerse desde el estado, además de involucrar a organizaciones sociales en esto. También, existen mecanismos de simplificación como el color, las fotos, las insignias partidarias, etc. que contribuyen a simplificar la operación de un equipo electrónico de votación.

- Pone en riesgo el secreto del sufragio: El secreto es algo que depende más del procedimiento de emisión del voto, que de la tecnología empleada. Prueba de ello es el sistema usado por redes clientelares, en el actual sistema, donde se entrega una boleta para sufragar con un número que los fiscales del partido anotan y que corresponde al emisor del voto, de este modo se sabe que la boleta entregada a un ciudadano fue utilizada en los comicios, y de ese modo se lo puede premiar por el voto emitido o castigarlo si la boleta que se le entregó no figura en la urna donde votó. El voto electrónico, responde a un programa, al que debe especificarle que no permita relacionar la emisión del voto con la persona que lo emite, tan simple como eso.
- Pone en riesgo la integridad del voto: Aquí se asocia el concepto de integridad a la materialización en papel del voto emitido, algo que en principio sería cuestionable, ya que el manejo de fondos de una cuenta bancaria, se realiza en forma electró-

nica, y el registro electrónico es el válido y no por ello se cuestiona al sistema de home banking por falta de materialidad o de integridad del dinero que maneja. La materialización o integridad de un registro electrónico, en este estadio de la tecnología me parece que no debería ser cuestionable; pero si así lo fuera, bastaría con emitir un comprobante en papel, del voto emitido, para dejar a salvo esa observación.

Privatiza el acto fundante de la democracia: Incluir la forma en que se materialice la implementación de los equipos de voto electrónico implica desconocer las múltiples opciones de producir un equipo de voto electrónico. Por ejemplo si las máquinas se produjeran en algún organismo del estado, con diseños públicos y con software público, con mecanismos para que cualquier organización política o social pueda auditar o verificar, en cualquier momento de su ciclo de vida tecnológico, no supone una privatización del acto electoral, sino todo lo contrario. Actualmente, en el proceso de envío del telegrama con los resultados de cada mesa y su proceso de recuento, intervienen computadoras, equipos de transmisión de datos y procesos no auditados ni verificados, donde solo que verifica mediante un simulacro, el funcionamiento del sistema.

Podemos concluir que las objeciones al voto electrónico, más que tecnológicas se centran en las metodologías de uso de la tecnología, la forma de adquirirla o administrarla. Por ello es innegable, que solo un amplio consenso que garantice las mayores facilidades de auditoría y fis-

calización puede ser viable, y esto no tiene contradicción alguna con el uso de la tecnología.

Para tener una idea, de los instrumentos tecnológicos, que se podrían utilizar en el sistema electoral, podríamos agruparlos según se utilicen en las distintas tareas del proceso electoral.

VI.1.- Etapa pre electoral

- Confección de padrones provisorios: las TICs aportarían elementos para simplificar su elaboración y depuración, puede citarse:
- La integración de las bases de datos de los registros de las personas, sobre todo a partir de las obtenidas con los nuevos documentos de identidad que aportan datos biométricos.
- La integración con las bases de datos del ANSES, que permitiría depurar por fallecimientos de personas, situación de empleo (para disponer de datos actualizados en la designación de autoridades de mesa), domicilio laboral (personas que tienen registrado un domicilio en una localidad y trabajan en otra muy distante).
- Integración con bases de datos de los partidos políticos (a los efectos de no designar a un afiliado a un partido como autoridad de mesa).
- Incorporación del correo electrónico en el padrón para uso de las autoridades electorales.
- Preselección de candidatos a autoridades de mesa, a fin de elaborar un listado público y que las personas puedan excusarse con anticipación.

- Incorporar un padrón digital al que se le agreguen datos biométricos para una identificación efectiva del votante, y quienes pueden ser elegidos autoridades electorales.

Publicación en un sitio web del padrón para que los ciudadanos tengan conocimiento de cómo figuran y puedan solicitar cambios (excusarse de ser autoridad electoral, cambio de domicilio).

- A partir de la incorporación de los datos biométricos se pueden generar terminales de auto gestión para la modificación de datos del padrón.
- Designación de autoridades de mesa: la designación realizada con el auxilio de los instrumentos propuestos en el inciso anterior permitiría:
- Elegir autoridades mediante un algoritmo computacional público, de código abierto y auditable; aplicado a la base de datos donde ya estarían preseleccionados las potenciales autoridades electorales.

Utilizar el correo electrónico para una primera notificación, pudiendo la autoridad designada concurrir a los terminales de autogestión para confirmar o solicitar su excusación.

Distribución de citaciones a autoridades de mesa:
la utilización de los instrumentos propuestos en los incisos anteriores permitiría:

- Las autoridades que fueron notificadas y aceptaron o se excusaron, no se incluirán en la notificación lo que reduciría y simplificaría el proceso de notificación tradicional.

- Debería mantenerse en vigencia el mecanismo de los terminales de autogestión, para los trámites de excusación y confirmación de la aceptación de la designación.

Envío de materiales a Secretarías electorales: la utilización de los instrumentos propuestos en los incisos anteriores permitiría:

- La utilización de envío electrónico de datos.
- Permitiría el control ciudadano de los trámites realizados si el proceso se comunica mediante su publicación en una página web (situación similar a la que se realiza con muchos trámites públicos)
- Aprobación de modelos de Boletas: la utilización de los instrumentos propuestos en los incisos anteriores permitiría:
- La comunicación entre las autoridades electorales y los partidos políticos se puede realizar vía acceso web y realizar estos trámites en forma digital.

Los modelos se pueden publicar en una página web de modo de estar disponibles para que cualquier ciudadano consulte.

Franquicia de distribución de boletas: la utilización de los instrumentos propuestos en los incisos anteriores permitiría que esto no sea necesario.

Impresión de padrones definitivos: la utilización de los instrumentos propuestos en los incisos anteriores permitiría:

- Contar con padrones digitales e impresos, lo que reduciría en mucho los costos de gráfica.

- Los padrones deberían dividirse en dos clases, uno público con información reducida que permita al votante y a cualquier ciudadano consultar donde se vota, si puede ser autoridad de mesa y si fue designado como autoridad. El padrón reservado conteniendo la información completa de los votantes (incluyendo los datos biométricos), solo debe circular cifrado y protegido con algún sistema de doble clave (similar al mecanismo utilizado por las transacciones de bitcoins).

Envío de padrones a Secretarías Electorales: la utilización de los instrumentos propuestos en los incisos anteriores permitiría:

- La utilización de envío electrónico de datos.
- Los padrones cifrados estarían solo disponibles, para su uso, por un número restringido de personas, todas identificadas y que dispondrán de una clave personalizada que lo identifique cada vez que acceda a los datos.

Distribución de financiamiento de campaña: la utilización de los instrumentos propuestos en los incisos anteriores permitiría:

- Publicar en un sitio web el mecanismo de otorgamiento de los fondos y la forma de aplicación de los partidos, poniendo a disposición de los ciudadanos la aplicación de los fondos públicos.

Distribución de espacios de Radio y TV, la utilización de los instrumentos propuestos en los incisos anteriores permitiría:

- Publicar en un sitio web el mecanismo de otorgamiento de los espacios y la forma que se utilizarán estos espacios por parte de los partidos, poniendo a disposición de los ciudadanos como se distribuye y utiliza el espacio publicitario.

Aprobación de pantallas de carga del recuento provisional: la utilización de los instrumentos propuestos en los incisos anteriores permitiría:

- Usar un software público, de código abierto y auditable.

Cierre del software de recuento provisional: la utilización de los instrumentos propuestos en los incisos anteriores permitiría que esto no sea necesario.

Deposito del software de recuento provisional: la utilización de los instrumentos propuestos en los incisos anteriores permitiría que esto no sea necesario.

Custodia de establecimientos de votación: la utilización de los instrumentos propuestos en los incisos anteriores permitiría:

- Incluir sistemas de vídeo vigilancia en la parte interna de los establecimientos (correspondiente a FFAA y de seguridad), combinados con las cámaras que posean los municipios (policías provinciales).
- Se podría generar un centro de vigilancia electoral, que centralice y coordine el uso de estas cámaras.

Entrega de materiales y documentación electoral: la utilización de los instrumentos propuestos en los incisos anteriores permitiría esto se realice de una manera totalmente distinta.

VI.2.- Etapa Electoral

Presentación de autoridades de mesa: la utilización de los instrumentos propuestos permitiría:

- La identificación de autoridades mediante sensores biométricos.
- La autenticación de los sistemas de uso en las mesas mediante sensores biométricos.
- El acceso a auditoria y verificación de sistemas, también por sensores biométricos.
- El uso de un sistema informático en lugar del sistema basado en papel.

Presentación de Fiscales de Mesa: la utilización de los instrumentos propuestos, permitiría:

- La identificación de fiscales mediante sensores biométricos
- La autenticación de los sistemas de uso en las mesas mediante sensores biométricos.
- El acceso a auditoria y verificación de sistemas también, por sensores biométricos.

Constitución Mesa, armado de urna, acondicionamiento del cuarto oscuro: la utilización de los instrumentos propuestos permitiría:

- El reemplazo del sistema de voto actual por una máquina de voto electrónico.
- La máquina de voto electrónico, cualquiera sea su modalidad (emisión y almacenamiento de voto, impresión de voto, sistema mixto de votación e impresión, etc.) se activa con los datos biométricos de las autoridades de mesa y los fiscales.

Identificación de los electores: la utilización de los instrumentos propuestos permitiría:

- La identificación de los electores mediante sensores biométricos.
- La publicación, en una página web, de quienes votaron.

Control de Boletas en cuarto oscuro: la utilización de los instrumentos propuestos en los incisos anteriores eliminaría esta tarea, pudiendo solo controlarse el normal funcionamiento de los equipos de voto electrónico.

Utilización de boletas de contingencia: la utilización de los instrumentos propuestos en los incisos anteriores eliminaría esta tarea.

Escrutinio de mesa: la utilización de los instrumentos propuestos permitiría:

- Un doble o triple sistema de verificación (conteo de la máquina de voto electrónico, conteo de voto impreso y conteo de impresión testigo en la máquina de voto electrónico).
- La definición de un procedimiento ágil y rápido de recuento y verificación.

Confección y suscripción e impresión de actas, certificados y telegramas: la utilización de los instrumentos propuestos permitiría:

- La confección de un acta digital encriptada y su respaldo en un documento impreso.
- El envío del acta digital desde la propia mesa de votación

Colocación de telegrama en sobre funda: la utilización

de los instrumentos propuestos en los incisos anteriores haría que esta tarea se aplique solo al respaldo impreso del acta de la mesa electoral.

Repliegue de materiales y documentación: la utilización de los instrumentos propuestos en los incisos anteriores implicaría que esta tarea se aplicaría a los equipos y sistemas utilizados en el acto electoral.

Custodia del repliegue de materiales y documentación: la utilización de los instrumentos propuestos en los incisos anteriores implicaría, que esta tarea se aplicaría a los equipos y sistemas utilizados en el acto electoral.

VII.3.- Etapa Post electoral

Llegada de telegrama a Centro de Digitalización Documental (CDD): la utilización de los instrumentos propuestos en los incisos anteriores permitiría:

- Permitir una validación on-line por parte de las autoridades y fiscales de mesa del acta, en CDD que actuaría como un nodo intermedio entre la mesa y el CPD.
- Distribuir copias de las actas a los centros de cómputos de los partidos participantes de los comicios y de los fiscales.
- Adicionalmente este trámite (no el resultado) podría volcarse en una página web.

Apertura de sobre funda en la CDD: la utilización de los instrumentos propuestos en los incisos anteriores restringiría esta tarea a una tarea de verificación de los datos del acta digital con la copia impresa.

Escaneo del telegrama en CDD: la utilización de los instrumentos propuestos en los incisos anteriores solo se utilizaría como respaldo digital de la copia impresa del acta.

Entrega electrónica del telegrama al Centro de Gestión de Datos (CGD): la utilización de los instrumentos propuestos en los incisos anteriores haría que esta tarea no fuera necesaria.

Seguimiento on-line del estado de la carga del telegrama en la CGD: la utilización de los instrumentos propuestos en los incisos anteriores haría que esta tarea no fuera necesaria.

Seguimiento on-line del estado de la carga del telegrama en el Centro de Procesamiento de Datos (CPD): la utilización de los instrumentos propuestos en los incisos anteriores haría que esta tarea no fuera necesaria ya que sería parte de un proceso ya iniciado anteriormente.

Publicación on-line de la imagen escaneada de cada telegrama: la utilización de los instrumentos propuestos en los incisos anteriores haría que esta tarea no fuera necesaria.

Depósito del software para su verificación: la utilización de los instrumentos propuestos, en los incisos anteriores, haría que esta tarea no fuera necesaria.

VI.1.- Escrutinio Definitivo

Detección de irregularidades en los cómputos provisorios: la utilización de los instrumentos propuestos en los incisos anteriores permitiría:

- Tener registro de cualquier irregularidad en el propio sistema (discrepancias entre el recuento

y el resultado de las máquinas de voto electrónico, problemas detectados en las verificaciones de equipos, etc.).

Control formal de actas: la utilización de los instrumentos propuestos en los incisos anteriores permitiría:

- Un control múltiple, ya que se puede auditar la máquina de voto electrónico, los comprobantes impresos o los comprobantes internos de la máquina, las actas digitales y los respaldos impresos.

Resolución de votos observados e impugnados: la utilización de los instrumentos propuestos en los incisos anteriores haría, que esta tarea no fuera necesaria, ya que sería resuelta en el inciso anterior.

Escrutinio por mesa: la utilización de los instrumentos propuestos en los incisos anteriores permitiría:

- Realizar el escrutinio definitivo mediante programas que interpreten las actas digitales, la copia impresa y la copia de la máquina de voto electrónico.

Ingreso de datos al sistema de Escrutinio definitivo: la utilización de los instrumentos propuestos en los incisos anteriores haría que esta tarea la realizara automáticamente el ítem anterior.

Aplicación del Sistema Electoral: la utilización de los instrumentos propuestos en los incisos anteriores haría que esta tarea se realice por la aplicación de un algoritmo computarizado, sujeto a aprobación de las autoridades electorales.

Proclamación de candidatos electos: no aplica aquí los instrumentos tecnológicos.

Los instrumentos propuestos no agotan, ni abarcan el universo de posibles aplicaciones tecnológicas que se podrían utilizar, pero puede ser un punto de partida para comenzar la discusión de su utilización. Por otra parte, los instrumentos tecnológicos por si solos no constituyen una solución, deben responder a una especificación que provenga de un consenso político entre las distintas fuerzas que suscriban esta solución, una vez acordado esto, deben especificarse los detalles de cada instrumento, su funcionamiento y su forma de uso. Por último debe adaptarse la normativa existente a la solución encontrada.

VII
PROPUESTA DE TRABAJO PARA EL DESARROLLO DE UN SISTEMA ELECTORAL

Si bien existen muchas formas de organizar el desarrollo de un sistema electoral, es necesaria una propuesta inicial, no para que se siga al pie de la letra, sino para tener un punto de partida a partir del cual definir una forma de trabajo definitiva.

VII.1.- Características

El desarrollo de un software para un sistema electoral, basándonos en los anteriores ítems debe como primera instancia definir los usuarios y su participación en el proyecto.

El usuario de un sistema electoral no es una persona, sino un conjunto de personas e instituciones. Las instituciones son el estado en sus tres estamentos:

- Poder ejecutivo: (quien no solo tiene la responsabilidad de soportar el proyecto, sino que es el responsable del acto eleccionario y principal usuario de las funcionalidades auxiliares del sistema las que debe especificar).
- Poder legislativo: es el responsable de especificar el sistema en conjunto con el ejecutivo, de controlar el proyecto y participar del mismo. También debe elaborar y/o aprobar el cuerpo normativo que regirá las prestaciones y las formas de uso del sistema.

- Poder Judicial: quien aporta el control y crea y tutela las aplicación de la normativa que incluye el uso del sistema.

Las instituciones de la sociedad civil:

- Partidos políticos: tienen la responsabilidad de especificar la forma, garantías, auditabilidad y la seguridad que debe garantizar el sistema. Puede participar de su desarrollo aportando auditores y desarrolladores.
- Los medios: La información que se maneja puede formar parte de la especificación del funcionamiento, la auditabilidad, la seguridad y las formas de difusión pública que tenga el sistema.
- Las organizaciones civiles: Las distintas organizaciones involucradas en el proceso electoral también pueden especificar la forma, garantías, auditabilidad y la seguridad que debe garantizar el sistema. Puede participar de su desarrollo aportando auditores y desarrolladores.
- El sistema nacional de C y T: Puede aportar su visión especializada en los procesos anteriores y ser uno de los partícipes fundamentales de las contribuciones técnicas para lograr un desarrollo con características innovadoras y de calidad.
- Un actor que debe ser tenido en cuenta es el elector individual que desee involucrarse a título personal en las distintas fases del proyecto, para lo cual debe preverse mecanismos de participación comunitaria en la gestión del proyecto.

VII.2.- Participantes

Los actores que deben participar del desarrollo del proyecto incluyen: personal en representación de los distintos sectores del poder ejecutivo, personal en representación de los distintos sectores del poder legislativo, personal en representación de los distintos sectores del poder ejecutivo, personal en representación de los partidos políticos, personal en representación de las distintos organizaciones de la sociedad civil, personal en representación de distintos medios de comunicación, personal del sistema nacional de C y T y particulares que se involucren en el proyecto.

Estos actores se distribuyen en distintas tareas que pueden agruparse en las siguientes categorías:

- Comité de dirección el proyecto: Reúne a representantes de todos los actores con responsabilidad política o legal en el desarrollo del proyecto. Es la máxima autoridad del proyecto en cuanto a la toma de decisiones generales del proyecto. De este comité depende el Director del proyecto y las aprobaciones finales de todas las decisiones trascendentes del proyecto.
- Dirección del Proyecto: Existe un solo director del proyecto que cuanta con un equipo de directores asociados en las distintas áreas del proyecto. De ellos dependen las decisiones operacionales del proyecto el control de los distintos equipos y la vinculación con los distintos comités del proyecto.
- Comité de especificación: Reúne a representantes

de todos los actores involucrados, organizados en comisiones que deberán en una primera instancia elaborar que requisitos debe cumplir el sistema. También, será responsable de las revisiones que se realicen con cada prueba unitaria y de proponer las reformulaciones que considere necesarias.

- Comité de planificación: Reúne a representantes de todos los actores involucrados, organizados en comisiones que revisan y auditan las tareas a realizar. Elaboran en conjunto con el Director del Proyecto las listas de tareas, el cronograma de tareas, las auditorías y participan del seguimiento del proyecto.
- Comité de Auditoría: Reúne a representantes de todos los actores involucrados, organizados en comisiones que realizan las pruebas unitarias, las auditorías que garanticen la total trasparencia del sistema y del proyecto de implementación.
- Comité de Vinculación y Transferencia: Reúne a representantes de todos los actores involucrados, organizados en comisiones que organizan la transferencia de los diseños realizados a sectores empresarios que lo construyan.
- Equipos de desarrollo: Reúne personal técnico que estén vinculados a los actores involucrados, organizados en equipos por áreas de trabajo. Son los responsables del desarrollo técnico del proyecto.
- Equipos de Documentación: Reúne personal técnico que esté vinculado a los actores involucrados, organizados en equipos por áreas de trabajo. Son

los responsables de la documentación del sistema.

- Equipos de Capacitación y Difusión: Reúne personal técnico que esté vinculado a los actores involucrados, organizados en equipos por áreas de trabajo. Son los responsables de la diseñar la capacitación de los distintos usuarios del sistema, y su difusión. Adicionalmente tendrá que organizar y mantener los contenidos de las páginas web del proyecto.
- Equipos de Seguridad: Reúne personal técnico que esté vinculado a los actores involucrados, organizados en equipos por áreas de trabajo. Son los responsables del diseño e implementación de la seguridad del sistema y del desarrollo. Adicionalmente tendrá la responsabilidad del desarrollo de la seguridad técnica de soporte a la seguridad física de los comicios.
- Equipos de Prueba: Reúne personal técnico que esté vinculado a los actores involucrados, organizados en equipos por áreas de trabajo. Son los responsables de realizar las pruebas unitarias, de funcionamiento y operación de los desarrollos que se realice en el proyecto. Dependerán del Director del proyecto, pero deben reportar los resultados de las pruebas al comité de auditoría.

Las áreas de trabajo que incluiría el proyecto son:

- Software operativo: Abarca todo el software de funcionamiento básico.
- Software gráfico: Abarca todo el software de presentación gráfica, captura y procesamiento de imágenes.

- Software de interface usuario: Abarca todo el software de comunicación con el usuario e impresión.
- Hardware y medios de soporte: Abarca todo lo relacionado con el hardware requerido para el funcionamiento del sistema.
- Integración de módulos: Abarca todo el software de integración de módulos, interfaces y configuración del hardware.
- Comunicaciones: Abarca todo lo relacionado con el hardware y software requerido para la comunicación del sistema, el proyecto y los soportes web.
- Encriptación y seguridad biométrica: Abarca todo lo relacionado con el hardware y software requerido para el funcionamiento de los sistemas de identificación de personas y la encriptación de la información.
- Seguridad: Abarca la seguridad del sistema, del proyecto y de los sistemas de soporte para la seguridad de los comicios.
- Auditoria y verificación: Abarca todo lo relacionado con la realización de pruebas dentro del proyecto, la realización de los procesos de auditorías y verificación del sistema y del proyecto.

VII.3.- Organización de los Participantes

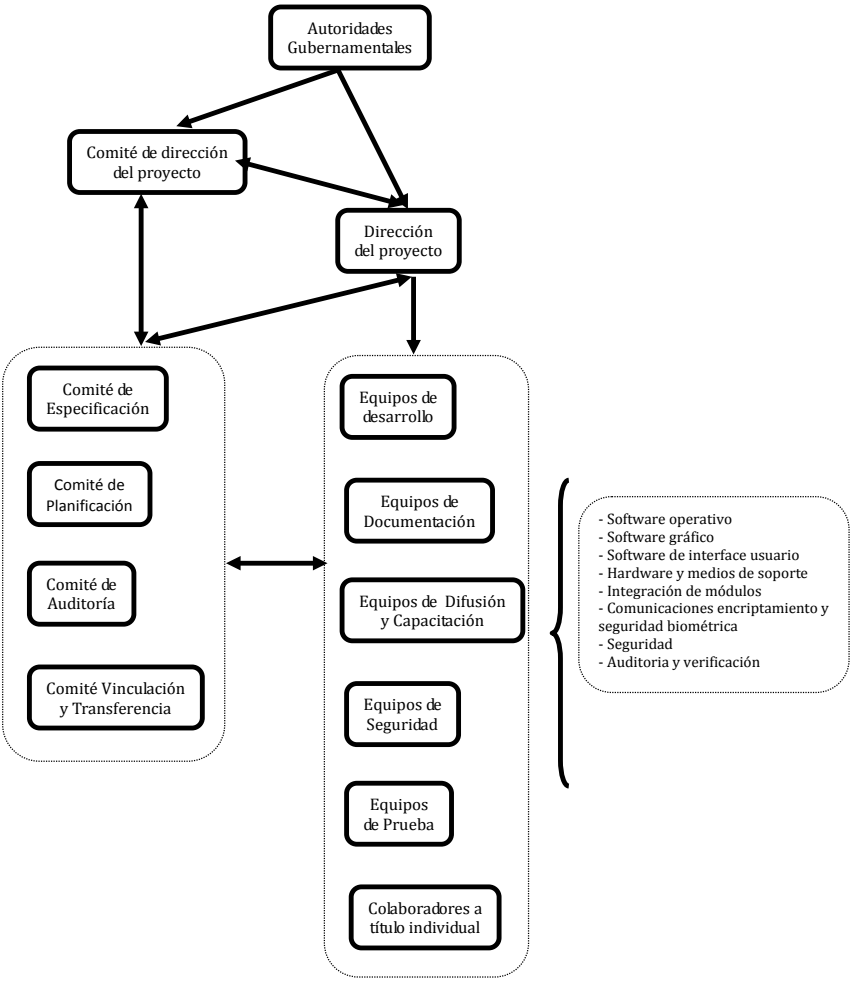
La organización se generaría a partir de una posible asignación por parte de las autoridades electorales respecto a quienes serían los responsables del proyecto en cuestión, se elegirían los miembros del Comité de Dirección del Proyecto y el Director del Proyecto, y este

conformaría su equipo de directores asociados. Sería recomendable la conformación de una dirección ejecutiva del proyecto.

La puesta en marcha requiere designar posteriormente los comités de especificación, auditoría y planeamiento, quienes se abocarían a la primera especificación (historia) y a la planificación de recursos y el cronograma inicial. En forma simultánea se organizarían los núcleos básicos de los distintos equipos de trabajo según las distintas áreas ya establecidas.

La primera aproximación al sistema se haría reuniendo las especificaciones iniciales y las distintas soluciones propuestas con aproximaciones (desarrollos RAD) y prototipos. Sobre esta base se ajustaría el cronograma y se completarían el comité de vinculación y transferencia, para que se inicien los contactos con las empresas que producirían los equipos.

Un esquema de cómo quedaría conformada la organización de los participantes del proyecto sería la siguiente:


Autoridades Gubernamentales
Comité de dirección del proyecto
Dirección del proyecto
Comité de Especificación
Comité de Planificación
Comité de Auditoría
Comité Vinculación y Transferencia
Equipos de desarrollo
Equipos de Documentación
Equipos de Difusión y Capacitación
Equipos de Seguridad
Equipos de Prueba
Colaboradores a título individual
- Software operativo
- Software gráfico
- Software de interface usuario
- Hardware y medios de soporte
- Integración de módulos
- Comunicaciones encriptamiento y seguridad biométrica
- Seguridad
- Auditoria y verificación

VIII
CONCLUSIONES Y RECOMENDACIONES

El presente trabajo analiza la naturaleza del voto electrónico, las experiencias en el mundo, Latinoamérica y Argentina, presentando una propuesta tecnológica y formato de organización para una implementación por parte del estado.

Sobre esto podemos concluir que el actual estado de la tecnología permite disponer de los elementos que garanticen la incorporación de tecnología en todo el proceso electoral (sistemas E2E), pero la factibilidad tecnológica no va de la mano con la confiabilidad que estos sistemas deberían inspirar, no tanto por su falibilidad sino por la posibilidad que se puedan alterar los resultados de la votación. El estado actual de la tecnología permite garantizar que es posible implementar cualquier sistema que cumpla las especificaciones que se le fijen desde el conjunto de las autoridades, los partidos políticos y las organizaciones de la sociedad civil. El total de las experiencias estudiadas en el presente trabajo evidencian esto; pero lo que no se puede es garantizar la confianza en los sistemas tecnológicos utilizados ya que estos son implementados por empresas privadas y el código de los programas utilizados no es de dominio público. Estas serían las dos primeras conclusiones que arroja el presente trabajo:

- Es posible garantizar la implementación tecnológica de cualquier propuesta sobre voto electrónico.
- Es imposible que esta implementación sea abso-

lutamente confiable si no se utiliza código abierto y público; participando el estado en todos sus estamentos y la sociedad civil, de la especificación y control de la implementación.

El análisis tecnológico de los distintos sistemas implementados permite asumir que cualquiera sea el sistema que adopte un país, el propio avance tecnológico podría hacer, en un lapso de tiempo no muy extenso, que este quede obsoleto. Por ello es necesario un estudio de la tecnología a emplear para que cualquier desarrollo que se intente poner en práctica no quede obsoleto antes de amortizar la inversión. Esta es otra conclusión a la que debe adicionarse a las anteriores:

- Las tecnologías empleadas en la integración del sistema de voto electrónico deben contemplar el horizonte de obsolescencia de dichas tecnologías para garantizar la amortización de la solución elegida.

Una segunda conclusión sobre aspectos tecnológicos del voto electrónico, y que surge del análisis de las experiencias realizadas por los distintos países, es que mayoritariamente participaron empresas privadas. Estas empresas tienen como objetivo prioritario la obtención de ganancias y no el interés público, por lo que es difícil compatibilizar una solución que satisfaga simultáneamente las necesidades de la sociedad y el rédito empresario. Un ejemplo de ello es la oferta, por parte de algunas empresas, de sistemas de voto electrónico con tecnologías que ya han sido superadas por otras. También se puede tomar como ejemplo la oferta de sistemas que cumplen especifi-

caciones de países con distinto marco legal y necesidades específicas. En función de esto puede concluirse que:

- La implementación de un sistema de voto electrónico debe surgir de las especificaciones propias del país que quiera implementarlo y no de la adaptación de un país a una oferta tecnológica proveniente de una empresa privada o de otro país.

Del análisis de las distintas experiencias en los países analizados podemos notar que los porcentajes de adopción del voto electrónico, son muy bajos en relación al total de países y también en referencia a la cantidad de países que han probado y realizado experiencias con él. Ahora bien, esto no significa que el voto electrónico no sea el sistema que termine adoptándose en un futuro, sino que este sistema se encuentra dentro de la llamada curva S de evolución de la tecnología, donde la tendencia inicial muestra un muy lento crecimiento de la adopción de la tecnología, luego al imponerse la tecnología se produce un rápido crecimiento de la adopción para amesetarse cuando la tecnología entra en obsolescencia. Por ello podemos concluir lo siguiente:

- El proceso de adopción de la tecnología electoral se encuentra a nivel mundial en su etapa inicial, aunque no se descarta que en un futuro no muy lejano se produzca un aumento considerable en el uso de esta tecnología.

Respecto de las actitudes que han tomado los actores políticos, judiciales y de la sociedad civil respecto al uso de la tecnología electoral en los casos analizados pode-

mos identificar tres tipos de conductas: la que busca la implementación del sistema de cualquier manera, la que mantiene una actitud crítica a favor de la adopción del voto electrónico y la que no considera que deba implementarse el voto electrónico. La primer conducta tiene una base voluntarista, generalmente impulsada por las circunstancias políticas que hacen necesario un cambio del sistema electoral debido a problemas de transparencia, igualdad de oportunidades y posibilidad de fraude de los sistemas tradicionales.

Las conductas opositoras al voto electrónico se pueden dividir en dos categorías: las surgidas por experiencias donde el sistema de voto electrónico utilizado falló o no satisfizo las expectativas; o por temor las fallas o al fraude que puede esconderse en un sistema del cual no se puede conocer totalmente su funcionamiento. Las conductas críticas a favor se basan en el reconocimiento de la existencia de una tecnología que finalmente se impondrá y la necesidad de poder asegurar el cumplimiento de las expectativas que genera el voto electrónico. Estas conductas nos llevan a la siguiente conclusión:

- La implementación de un sistema de voto electrónico debe impedir conductas voluntaristas que pretendan su adopción de cualquier modo, garantizar una respuesta satisfactoria a todo cuestionamiento sobre el correcto funcionamiento y la imposibilidad de fraude en el uso del sistema; e incluir todas las sugerencias que se hagan para su adopción.

Dos experiencias analizadas, la de Canadá y la de India, nos muestra que es posible realizar un sistema voto electrónico utilizando software de código abierto y hallar un sistema confiable de costo razonable. En el caso de Canadá, el sistema fue desarrollado por una empresa privada bajo especificaciones de las autoridades gubernamentales, en un plazo de seis meses. En India, el sistema utilizado, también bajo directivas gubernamentales, tuvo un costo de aproximadamente u$a 300, por terminal de voto electrónico. Por lo tanto podemos concluir:

- Es posible el desarrollo de un sistema de voto electrónico económico y basado en software de código abierto o software libre.

Estas conclusiones nos permiten sugerir que cualquier proceso de adopción de la tecnología de voto electrónico debería basarse en un amplio consenso de todos los actores políticos, jurídicos y de la sociedad civil. El consenso debería darse en términos de las garantías que se deben satisfacer para que todas las partes acuerden incorporar un sistema de voto electrónico. Los pasos que deberían darse en ese proceso serían:

1. Definir las garantías debe dar el sistema de voto electrónico: Todos los sectores deben explicitar las condiciones que debería tener el sistema para no generar, a su criterio, ninguna duda sobre el funcionamiento del sistema de voto electrónico y los resultados que éste produzca.
2. Definir que tecnologías se incorporarán al sistema electoral: La existencia de varias tecnologías con las

que se puede integrar el sistema de voto electrónico debe ser definido, entre los actores ya mencionados y distintos expertos que los asesoren.

3. Definir la forma en que se implementará: La construcción de los sistemas a utilizar es algo que debe ser consensuado por todos los actores o quienes estos designen que el proceso de fabricación o desarrollo cumpla y no altere lo especificado.
4. Definir los mecanismos de verificación en la implementación del sistema: La construcción de los sistemas a utilizar es algo que debe ser verificado por todos los actores o quienes estos designen para garantizar que el proceso de fabricación o desarrollo cumpla lo establecido.
5. Definir los mecanismos de utilización del sistema: El sistema electoral elegido no solo debe ser especificado en su funcionamiento y fabricación o desarrollo, sino también en su operación por lo que deben definirse los procesos a realizar para la operación del sistema.
6. Definir los mecanismos de verificación de la utilización del sistema: El uso del sistema de voto electrónico que fue consensuado debe contar con mecanismos de verificación definidos previamente.
7. Definir mecanismos de arbitrio de diferencias: Dada la imposibilidad de acordar previamente todos los detalles, pueden surgir a posteriori diferencias no previstas sobre aspectos del sistema, para lo cual es necesario contar con mecanismos de solución de esas diferencias.

8. Definir mecanismos de procedimientos ante fallas: El sistema y su operación no están libres de fallas, razón por la cual estas deben preverse previamente.

Ante esto las recomendaciones que se sugieren son las siguientes:

- El sistema a utilizar debe surgir del mayor consenso posible (ver inciso VIII).
- Del mismo consenso debe surgir un sistema lo más actualizado tecnológicamente e implementado con programas de código abierto (Ver anexo A).
- El sistema debe implementar un proceso E2E para darle la mayor fiabilidad posible (ver anexo C).
- Sería deseable que el sistema se desarrollara en el país y se transfiera a empresas locales para su mantenimiento y operación; y que organismos del estado se encargasen de su estudio, mejora y actualización.
- De ser posible sería deseable el desarrollo de un prototipo experimental previo
- De ser posible la fabricación o desarrollo debería realizarse con la participación conjunta de empresas privadas y organismos del estado.

Si bien estas recomendaciones no son indispensables es casi seguro que llevarlas a cabo redundaría en la adopción de un sistema de votación útil y confiable.

ANEXO A
SOFTWARE LIBRE: IMPRESCINDIBLE PARA EL SISTEMA DE VOTO ELECTRÓNICO

Una característica que debe tener un sistema de voto electrónico, es el uso de programas cuyo código esté disponible para que todos puedan examinarlo y proponer mejoras. Esta, es la principal característica del Software Libre (SL). Sin esto nadie puede asegurar que los programas usados por el sistema no contengan rutinas que puedan alterar o poner en riesgo la seguridad del voto electrónico.

Software Libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. De modo más preciso, se refiere a cuatro libertades de los usuarios del software, expresados por Stallman (STALLMAN, 2005) :

La libertad de usar el programa, con cualquier propósito (libertad 0).

La libertad de estudiar cómo funciona el programa, y adaptarlo a sus necesidades (libertad 1).El acceso al código fuente es una condición previa para esto.

La libertad de distribuir copias, con lo que puedes ayudar a tu vecino (libertad 2).

La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie (libertad 3). El acceso al código fuente es un requisito previo para esto.

Un programa es software libre si los usuarios tienen todas estas libertades. Así pues, se debería tener la libertad de distribuir copias, sea con o sin modificaciones, sea gratis o cobrando una cantidad por la distribución, a cualquiera y a cualquier lugar. El ser libre de hacer esto significa (entre otras cosas) que no se tiene que pedir o pagar permisos. También, se debería tener la libertad de hacer modificaciones y utilizarlas de manera privada en el trabajo u ocio, sin ni siquiera tener que anunciar que dichas modificaciones existen. Si se publican los cambios, no se tiene por qué avisar a nadie en particular, ni de ninguna manera en particular.

La libertad para usar un programa significa la libertad para cualquier persona u organización de usarlo en cualquier tipo de sistema informático, para cualquier clase de trabajo, y sin tener obligación de comunicárselo al desarrollador o a alguna otra entidad específica.

La libertad de distribuir copias debe incluir tanto las formas binarias o ejecutables del programa como su código fuente, sean versiones modificadas o sin modificar (distribuir programas de modo ejecutable es necesario para que los sistemas operativos libres sean fáciles de instalar). Está bien si no hay manera de producir un binario o ejecutable de un programa concreto (ya que algunos lenguajes no tienen esta capacidad), pero se debe tener la libertad de distribuir estos formatos si se encontrara o desarrollara la manera de crearlos.

Para que las libertades de hacer modificaciones y de publicar versiones mejoradas tengan sentido, se debe te-

ner acceso al código fuente del programa. Por lo tanto, la posibilidad de acceder al código fuente es una condición necesaria para el software libre.

Para que estas libertades sean reales, deben ser irrevocables mientras no se haga nada incorrecto; si el desarrollador del software tiene el poder de revocar la licencia aunque no se le haya dado motivos, el software no es libre.

Son aceptables, sin embargo, ciertos tipos de reglas sobre la manera de distribuir software libre, mientras no entren en conflicto con las libertades centrales. Por ejemplo, "copyleftes" la regla que implica que, cuando se redistribuya el programa, no se pueden agregar restricciones para denegar a otras personas las libertades centrales. Esta regla no entra en conflicto con las libertades centrales, sino que más bien las protege.

Software Libre no significa "no comercial". Un programa libre debe estar disponible para uso comercial, desarrollo comercial y distribución comercial. El desarrollo comercial del software libre ha dejado de ser inusual; el software comercial libre es muy importante.

Pero el software libre sin `copyleft' también existe. Creemos, que hay razones importantes por las que es mejor usar 'copyleft', pero si los programas son software libre sin ser 'copyleft', se lo puede utilizar de todos modos.

Cuando se habla de software libre, es mejor evitar términos como: `regalar' o `gratis', porque esos términos implican que lo importante es el precio, y no la libertad.

El SL posee un sinnúmero de ventajas entre ellas, podemos señalar:

- Económico: El bajo o nulo coste de los productos libres permiten proporcionar servicios y ampliar infraestructuras sin pagar grandes cantidades en licencias. Además, de la reducción de costes por uso de software libre. ¿Qué podrían aportar esas inversiones si los beneficiados fuesen empresas del propio estado, en lugar de mandar a una compañía extranjera esas enormes cantidades de dinero?
- Libertad de uso y redistribución: Las licencias de software libre existentes, permiten la instalación del software tantas veces y en tantas máquinas como el usuario desee.
- Independencia tecnológica: El acceso al código fuente, permite el desarrollo de nuevos productos sin la necesidad de desarrollar todo el proceso partiendo de cero. El secretismo tecnológico es uno de los grandes frenos y desequilibrios existentes para el desarrollo en el modelo de propiedad intelectual.
- Fomento de la libre competencia al basarse en servicios y no licencias: Uno de los modelos de negocio, que genera el software libre, es la contratación de servicios de atención al cliente. Este sistema permite, que las compañías que den el servicio compitan en igualdad de condiciones al no poseer la propiedad del producto del cual dan el servicio.
- Soporte y compatibilidad a largo plazo: Este punto, más que una ventaja del software libre es una desventaja del software propietario, por lo que la elección de software libre evita este problema. Al vendedor, una vez ha alcanzado el máximo de ven-

tas que puede realizar de un producto, no le interesa que sus clientes continúen con él. La opción es sacar un nuevo producto, producir software que emplee nuevas tecnologías solo para éste y no dar soporte para la resolución de fallos al anterior, tratando de hacerlo obsoleto por todos los medios, pese a que este pudiera cubrir perfectamente las necesidades de muchos de sus usuarios. Véanse diferentes versiones de Windows, que dejan de ser soportadas por Microsoft, o software de grabación que no admite nuevos modelos de grabadoras ópticas sin una actualización, aún cuando la grabadora nueva emplee el mismo mecanismo de grabación que la antigua.

- Formatos estándar: Los formatos estándar permiten una interoperatividad más alta entre sistemas, evitando incompatibilidades. Los estándares de facto son válidos en ocasiones para lograr una alta interoperatividad, si se omite el hecho que estos exigen el pago de royalties a terceros y por razones de mercado, expuestas en el anterior punto, no interesa que se perpetúen mucho tiempo. Los formatos estándares afectan a todos los niveles. Un ejemplo lo estamos viendo en los documentos emitidos por las administraciones públicas en distintos formatos y versiones, que producen retrasos y dificultades en el acceso adecuado a la información para las mismas administraciones y para sus usuarios. Algunas administraciones de la unión europea ya están dando el paso a formatos abiertos como ODF

(Open Document Format).

- Sistemas sin puertas traseras y más seguros: El acceso al código fuente permite, que tanto hackers como empresas de seguridad de todo el mundo puedan auditar los programas, por lo que la existencia de puertas traseras es ilógica ya que se pondría en evidencia y contraviene el interés de la comunidad que es la que lo genera.
- Corrección más rápida y eficiente de fallos: El funcionamiento e interés conjunto de la comunidad ha demostrado solucionar más rápidamente los fallos de seguridad en el software libre, algo que desgraciadamente en el software propietario es más difícil y costoso. Cuando se notifica a las empresas propietarias del software, éstas niegan inicialmente la existencia de dichos fallos por cuestiones de imagen y cuando finalmente admiten la existencia de esos bugs tardan meses hasta proporcionar los parches de seguridad.
- Métodos simples y unificados de gestión de software: Actualmente, la mayoría de distribuciones de Linux incorporan alguno de los sistemas que unifican el método de instalación de programas, librerías, etc. por parte de los usuarios. Esto llega a simplificar hasta el grado de marcar o desmarcar una casilla para la gestión del software, y permiten el acceso a las miles de aplicaciones existentes de forma segura y gratuita a la par que evitan tener que recurrir a páginas web de dudosa ética desde las que los usuarios instalan sin saberlo spyware o

virus informáticos en sus sistemas. Este sistema de acceso y gestión del software se hace prácticamente utópico si se extrapola al mercado propietario.

- Sistema en expansión: Las ventajas especialmente económicas que aportan las soluciones libres a muchas empresas y las aportaciones de la comunidad han permitido un constante crecimiento del software libre, hasta superar, en ocasiones como en el de los servidores web, al mercado propietario.

El software libre ya no es una promesa, es una realidad y se utiliza en sistemas de producción por algunas de las empresas tecnológicas más importantes como IBM, SUN Microsystems, Google, Hewlett-Packard, etc. Paradójicamente, incluso Microsoft, que posee sus propias herramientas, emplea GNU Linux en muchos de sus servidores.

A.1.- CÓMO ES EN GENERAL LA GESTIÓN DE UN PROYECTO DE SOFTWARE LIBRE

La gestión de proyectos es la disciplina que agrupa y ordena el conjunto de tareas o actividades destinadas a obtener objetivos. Para esto hay varias tareas, que incluyen: planificación, definición, ordenamiento y gestión de las actividades que formarán el proyecto software. Una buena gestión es la que es capaz de reducir al mínimo las posibilidades de fallo, entendiendo por esto, no obtener los requisitos iniciales del proyecto, la inviabilidad económica del mismo, un resultado que impida mantenerlo o le impida evolucionar, etc. Otra visión más orientada a lo económico, es la que define la buena gestión, como la

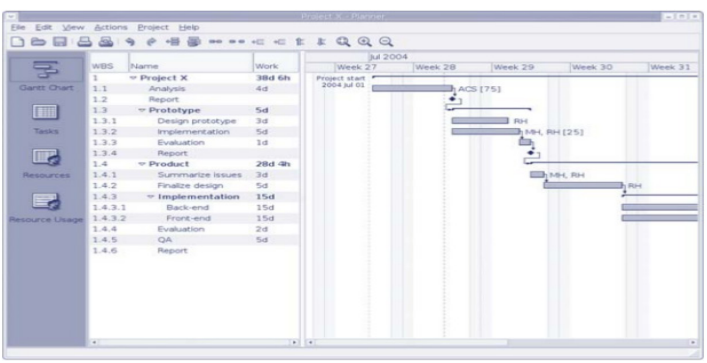
que optimiza el uso de los recursos de tiempo, dinero, personas, equipos, etc., en cada fase del proyecto.

Comúnmente, la responsabilidad de la gestión del proyecto la tiene el director del proyecto, que no tiene por qué participar activamente en las actividades del mismo, pero que sí se ocupa de monitorizar su progreso y de la interacción entre los diferentes grupos que intervienen en éste para minimizar el riesgo de fallo del proyecto.

A.1.1.- Qué herramientas se usan en la gestión

Una de las principales herramientas de la gestión son los diagramas de Gantt, son muy usados en estos entornos por mostrar de una forma clara la sucesión de tareas, recursos involucrados y sus dependencias.

En los diagramas de Gantt, representamos las actividades que hay que realizar en forma de árbol (mitad izquierda de la figura), indicando su fecha de inicio y su duración estimada. El programa representa la actividad sobre un calendario (mitad derecha de la figura) y nos



permite definir las dependencias entre las actividades. Al indicar que una tarea debe empezarse al terminar otra, o que deben empezar a la vez o terminar las dos simultáneamente, el diagrama va modificando automáticamente la situación de las actividades en el tiempo.

El camino crítico de un proyecto se define como la secuencia de tareas que suman el intervalo de tiempo más largo del mismo. Así pues, determina la duración mínima del proyecto, ya que un retraso en alguna de sus tareas tiene un impacto directo en su duración total. Dependiendo de la complejidad del programa que utilicemos para representar el diagrama, podremos especificar también los recursos disponibles, los necesarios para cada tarea, etc. y seremos capaces de detectar conflictos en la planificación, como intervalos en los que no dispondremos de los recursos necesarios, o cuál va a ser el camino crítico del proyecto.

A.1.2.- Qué sucede en el desarrollo de Software Libre

En entornos de software libre, no existe una forma "tradicional" de gestionar un proyecto. Un buen ejemplo de ello es el artículo de Eric S. Raymond, "La Catedral y el Bazar", en el que se describe la forma tradicional de gestionar un proyecto como analogía de construir una catedral, y se compara la forma como se gestionan muchos proyectos de software libre al funcionamiento de un bazar. Proyectos grandes de software libre, como el desarrollo del núcleo Linux o el servidor web Apache, están formados por un comité de gestión del proyecto o una sola persona (que puede tener un comité ad hoc) que de-

ciden los siguientes pasos que habrá que llevar a cabo en el proyecto, y que inmediatamente delegan en otras personas o equipos los trabajos a realizar para alcanzar los objetivos. La aprobación de los trabajos, cambios o modificaciones que se realizan al proyecto original sigue el proceso inverso hasta llegar a su aprobación.

En este tipo de gestión de proyectos, juega un papel fundamental las herramientas de soporte y comunicación entre los diferentes equipos. Programas de gestión de incidencias como el conocido Bugzilla o entornos como Sourceforge, ayudan a los gestores del proyecto o a los comités organizadores a conocer el estado del proyecto, la opinión de sus usuarios, las aportaciones de los desarrolladores, etc.

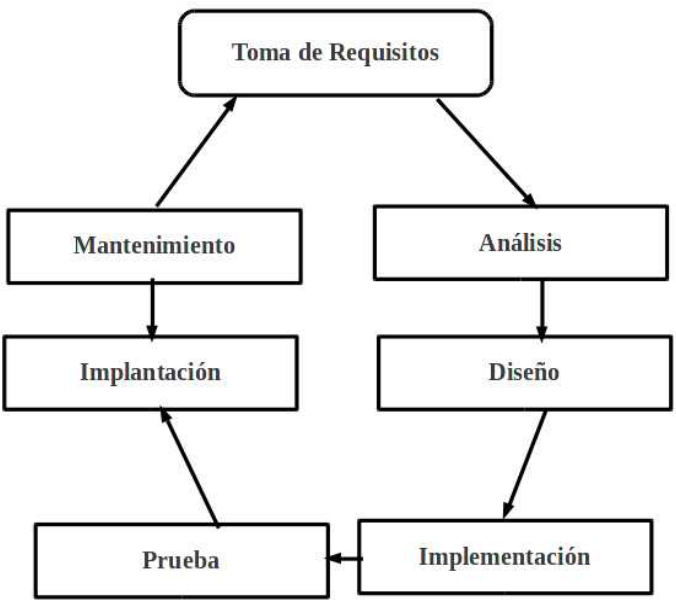
En todos los proyectos de software libre no se acostumbra seguir una metodología rígida y se orientan más a una gestión ágil, siguiendo principios acordes con el software libre. En la dirección de proyectos de envergadura, el director no suele intervenir directamente en el desarrollo y la mayoría de actividades, a diferencia de lo que ocurre en pequeños proyectos.

A.2.- FORMAS DE GESTIÓN DEL DESARROLLO DE SOFTWARE

Existen distintas formas de plantear el desarrollo de un software, la teoría clásica supone una seria de actividades relacionadas entre sí, a las que se denominan modelos de desarrollo de software. Los modelos se basan en el Ciclo de vida del software. Se llama así a las fases por las que pasa un proyecto software desde que es concebi-

do, hasta que está listo para usarse. Típicamente, incluye las siguientes actividades: toma de requisitos, análisis, diseño, desarrollo, pruebas (validación, aseguramiento de la calidad), instalación (implantación), uso, mantenimiento y obsolescencia.

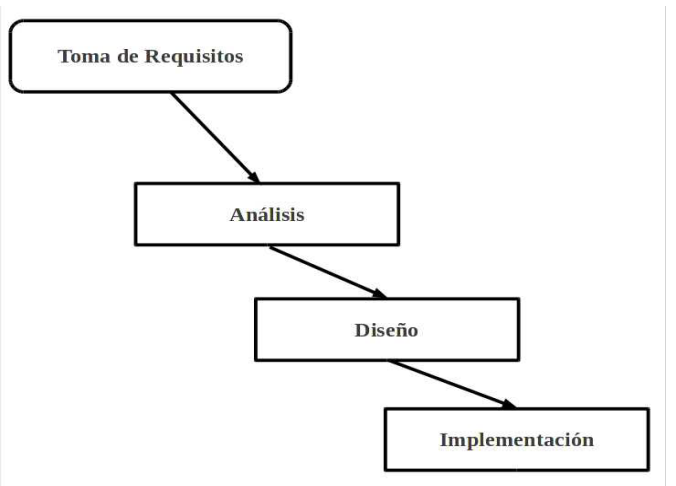
Un proyecto tiende a pasar iterativamente por estas fases, en lugar de hacerlo de forma lineal. Así pues, se han propuesto varios modelos (en cascada, incremental, evolutivo, en espiral, o concurrente, por citar algunos) para describir el progreso real del proyecto.



A.2.1.- Modelo Cascada

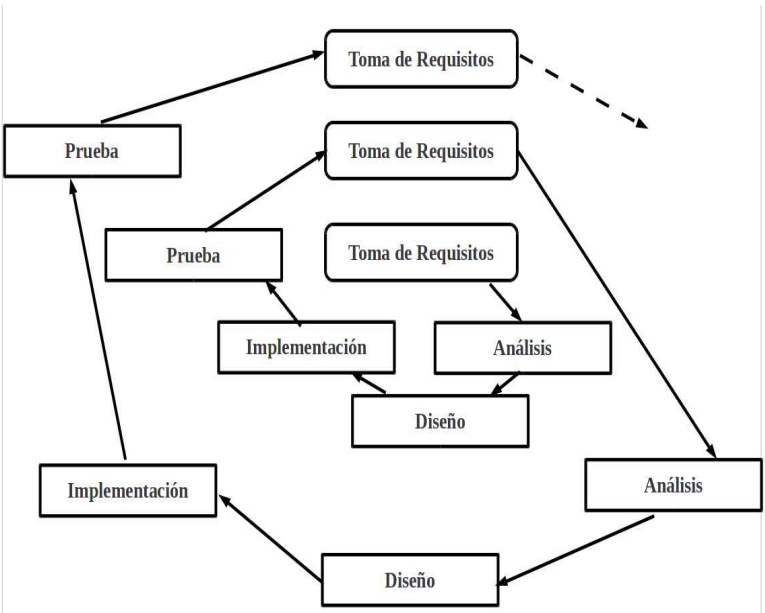
Este modelo es el más simple y sirve de base para el resto. Simplemente asigna unas actividades a cada fase, que servirán para completarla y para proporcionar los requisitos de la siguiente. Así, el proyecto no se diseña hasta que ha sido analizado, o se desarrolla hasta que ha sido diseñado, o se prueba hasta que ha sido desarrollado, etc.

Los otros modelos son una variación del modelo en cascada en la que éste se aplica a subconjuntos del proyecto. Dependiendo de si los subconjuntos son partes del total (modelo incremental) o bien versiones completas, pero con menos prestaciones (modelo evolutivo) se estará aplicando uno u otro.



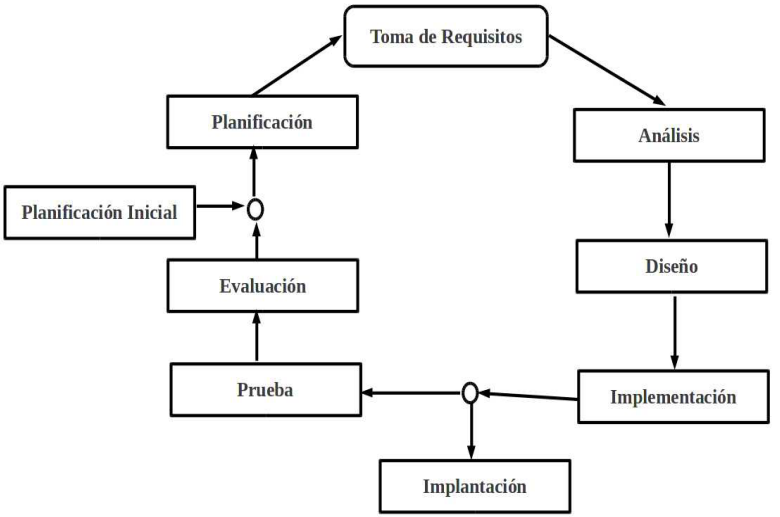
A.2.2.- Modelo Espiral

Este modelo se basa en la creación de prototipos del proyecto, que pasan por las fases anteriores, y que van acercándose sucesivamente a los objetivos finales. Así, nos permite examinar y validar repetidamente los requisitos y diseños del proyecto antes de acometer nuevas fases de desarrollo.



A.2.3.- Modelo Iterativo o Incremental

Este modelo permite que las fases de análisis, diseño, desarrollo y pruebas se retroalimenten continuamente, y que empiecen lo antes posible. Permitirá atender a po-



sibles cambios en las necesidades del usuario o a nuevas herramientas o componentes que los desarrolladores descubran y que faciliten el diseño o proporcionen nuevas funcionalidades.

Se trata de obtener lo más rápidamente una versión funcional del software, y añadirle prestaciones a partir de lo que se ha aprendido en la versión anterior. El aprendizaje proviene tanto del desarrollo anterior, como del uso del software, si es posible. En este tipo de desarrollo es imprescindible establecer una lista de control del proyecto, donde iremos registrando las funcionalidades que faltan por implementar, las reacciones de los usuarios, etc. y que nos proporcionará las bases para cada nueva iteración. Este último método es el más usado (aunque

sea involuntariamente) en proyectos de software libre, por la propia naturaleza cambiante de los requisitos o la aportación constante de nuevos colaboradores.

A.2.4.- DESCRIPCIÓN DE LAS ACTIVIDADES BÁSICAS DEL DESARROLLO

Los distintos modelos plantean las mismas actividades, pero vinculadas de distinto modo y con distintas intensidades. Un breve resumen de cómo se realizan esas actividades permite, una mayor comprensión de cómo se desarrollará el proyecto.

A.2.4.1.- Análisis de requisitos

El análisis de requisitos es la primera fase de la vida de un proyecto. En ella, habrá que recoger tanto las necesidades del usuario del producto, al más alto nivel, como la especificación de los requisitos software del sistema. Para guiarnos en ese proceso, existen multitud de plantillas, libros y metodologías orientados a extraer del usuario lo que realmente quiere que haga el sistema. Sin duda, no es una tarea sencilla. Existen disponibles en Internet plantillas de documentos para la gestión de un proyecto de desarrollo software. Siguiendo estas plantillas, vemos que la especificación de requisitos del sistema incluye, como mínimo:

- Los casos de uso: actores que intervendrán en el uso del producto y sus posibles acciones.
- Sus requisitos funcionales: prestaciones del sistema de software en la primera versión y posible planificación para las futuras versiones.

Sus requisitos no funcionales: de rendimiento, de usabilidad, de seguridad, etc.

En entornos de software libre, muy frecuentemente el director del proyecto será también su primer usuario, determinará el alcance del proyecto en sus primeras versiones, y permitirá que nuevos desarrolladores se vayan incorporando al proyecto. Esto se complementa con el control del progreso y objetivos del proyecto.

A.2.4.2.-Estimación de costes

La estimación de costes (recursos, equipos y tiempo empleado) es una de las razones de ser de la ingeniería del software. Aunque no siempre se aplica en desarrollos de software libre, es conveniente conocer las métricas y métodos que nos permitirán predecir el esfuerzo que supondrá implementar un sistema o alguna de sus prestaciones.

La estimación suele realizarse basándose en modelos matemáticos que parten del "tamaño" estimado del proyecto, y de constantes que lo ajustan según las tecnologías usadas, recursos de que disponemos, etc. Los modelos nos permiten estimar el esfuerzo requerido (habitualmente en horas/hombre o meses/hombre) para terminar el proyecto. Obviamente, la clave está en estimar el "tamaño" del proyecto. Otros modelos usan los denominados "puntos de función", que son una medida de la complejidad de cada funcionalidad a partir de las entradas que recibe, las salidas que aporta, su interacción con otras funcionalidades o recursos, etc.

Existen también otras métricas, que tienen en cuenta factores como los métodos por clase, las herencias entre

objetos, la interacción entre ellos, su grado de dependencia (que complica el mantenimiento, etc.). No es muy importante para el proyecto de software libre un conocimiento exhaustivo de estos conceptos, sino su aplicación a los efectos de completar una adecuada planificación del proyecto.

A.2.4.3.-Diseño

La fase de diseño del sistema producirá un conjunto de documentos que describirán un sistema que cumpla con los objetivos de la fase de análisis de requisitos. Las decisiones que se tomen en esta fase deberán basarse en esos requisitos y en la comprensión de la tecnología y los componentes disponibles.

Debe tenerse en cuenta que muchos de los documentos que se crearán en esta fase van a usarse por los desarrolladores del proyecto (diagramas de componentes del sistema, arquitectura del mismo, etc.). Esto implica que deben hacerse lo más completos posible, y que la participación de los desarrolladores en esta fase ayudará a evitar revisiones innecesarias. Otros documentos irán destinados a los usuarios del proyecto (p. ej., el diseño de la interfaz de usuario), y su aprobación y entendimiento de éstos también será clave para evitar desviaciones. Por todo ello, es muy conveniente disponer de listas que nos permitan comprobar que no hemos olvidado ningún aspecto clave en esta fase. Entre los documentos más significativos, encontramos:

- Diagrama estructural: diseño y notas sobre la estructura del sistema en detalle.
- Diagrama de comportamiento: diseño y notas sobre el comportamiento del sistema.

- Arquitectura del sistema: diseño de sus componentes, de su implantación e integración.
- Organización de código fuente y compilación: Directorios, opciones de compilación, sistemas de control de versiones, etc.
- Interfaz de usuario: metáforas, estándares a seguir, diseño de los contextos de interacción con el usuario, etc.
- Sistema de información: bases de datos, abstracción de objetos, almacenamiento, persistencia, etc.
- Seguridad.

A.2.4.4.-Documentación

La documentación de un proyecto es de vital importancia para su éxito, desde la fase de diseño, como parte de la propia arquitectura del proyecto, se debe definir y escoger el sistema de documentación que se usará para el proyecto, teniendo en cuenta factores como los siguientes:

Formatos de los documentos, según su tipología y métodos de acceso. Se debe definir los formatos y plantillas elegidos para los diagramas de diseño, hojas de cálculo, hojas de seguimiento del proyecto, documentos que registren fallos o cambios en las especificaciones durante el desarrollo, documentos que definan la interfaz de usuario, etc.

Método de acceso y flujo de trabajo de cada tipo de documento. Quién va a tener acceso a los diferentes tipos de documentos y bajo qué privilegios. Dónde se van a notificar los cambios que se realicen (¿en el propio documento?, ¿en un sistema de control de versiones?).

En el caso de la documentación del código fuente del proyecto, conviene estudiar las herramientas que ofrezca el propio lenguaje para generar la documentación, ya que en muchos casos existen herramientas de generación de documentación a partir del código fuente y comentarios insertados mediante una sintaxis determinada que van a ayudar mucho en el proceso.

En el momento de tomar decisiones de formato y flujos de trabajo sobre la documentación, es de vital importancia tener en cuenta los estándares de formatos de documento existentes, evitando los formatos propietarios sobre todo en organizaciones heterogéneas donde convivan distintos sistemas operativos o en proyectos de software libre, para dar a la documentación la mayor accesibilidad posible. Suele ser una buena decisión escoger un formato de documentación fácilmente convertible a otros (p.ej., XML) y así poder disponer de la documentación en HTML para su consulta rápida, en PDF para agregar a la documentación del proyecto, etc.

A.2.4.5.-Pruebas y calidad

Para que un proyecto software tenga éxito, es necesario que el resultado cuente con la calidad esperada por el usuario. Así pues, la calidad del proyecto deberá poderse definir en términos de prestaciones, respuestas esperadas a determinadas acciones, o accesibilidad del producto en diferentes condiciones para poder probarla posteriormente mediante test de calidad específicos.

Deberá ser posible realizar un plan de pruebas o de aseguramiento de la calidad que clasifique las activida-

des relacionadas con la calidad del producto según su importancia, y que defina con qué frecuencia y qué resultados se deberían obtener de cada una para pasar a la siguiente o para cumplir los requisitos para esa release en particular. El proceso de aseguramiento de la calidad no trata únicamente de que el producto pase todos los tests establecidos, sino que implicará:

- El uso de hojas de estilo aprobadas por los usuarios.
- La confección y repaso de check-lists sobre funcionalidades.
- La revisión periódica del producto con los usuarios.
- Las herramientas que pondremos a disposición de los usuarios para comunicar los errores o sugerencias.

El uso de herramientas de análisis para medir la respuesta del proyecto a determinadas situaciones, o para simular un uso normal del mismo.

Los modelos tradicionales de ciclo de vida del software incluían la fase de pruebas como un proceso, que había que llevar a cabo, una vez finalizado el desarrollo, esto resulta altamente contraproducente, no sólo por el coste de arreglar fallos o deficiencias una vez terminado el desarrollo, sino por la naturaleza evolutiva de muchos proyectos.

Así, se tiende a incorporar las pruebas, o los mecanismos para llevarlas a cabo de modo automatizado, desde el primer momento. Tecnologías como las pruebas unitarias o modelos como el pair-programming o el peer-testing nos ayudarán a mantener una disciplina en el desarrollo y a aumentar la calidad del resultado del proyecto.

A.2.4.6.-Seguridad

La seguridad en proyectos software ha sido un factor clave desde el inicio de la ingeniería del software. Igual que en otros conceptos como la calidad, la seguridad no puede ser un módulo en el diseño que tiene lugar fuera de él, ni un proceso que se comprueba al finalizar el desarrollo, sino que se trata de un aspecto del proyecto que tiene que tenerse en cuenta y planificarse desde la fase de diseño, y que afectará a lo largo de todo el ciclo de vida del proyecto. Los principios básicos de la seguridad de un sistema son los siguientes:

- Confidencialidad: los recursos (o funcionalidades sobre ellos) son accesibles sólo para los usuarios (o procesos) autorizados.
- Integridad: los recursos pueden ser modificables sólo por los usuarios autorizados.

Disponibilidad: los recursos accesibles están disponibles.

Muy frecuentemente, la seguridad de un proyecto irá más allá del mismo, afectando al sistema en el que éste se va a implantar, y por lo tanto deberemos asegurar que su implantación deja al sistema final en un estado seguro.

Es por esta razón por lo que, en la fase de diseño del proyecto, se debe tener en cuenta la seguridad del mismo, primero de forma general mediante un análisis de riesgos y de actividades destinadas a mitigarlos, y más adelante mediante la ampliación de los casos de uso según los principios básicos de la seguridad comentados anteriormente. El análisis de riesgos consistirá, de forma muy resumida, en las siguientes actividades:

- Recopilación de los recursos que deben ser protegidos. La información, todo un sistema, un sólo dispositivo, etc.

Clasificación de los actores del proyecto. Cuáles son sus casos de uso y qué roles representan.

Recopilación de requisitos legales y de negocio. Certificaciones que hay que cumplir, restricciones de encriptación por exportación a determinados países o bien reglas de negocio más específicas como la aceptación o no de la repudiación por parte de los usuarios.

Con la información recopilada, deberíamos ser capaces de construir una tabla en la que, para cada riesgo, estimáramos el coste que tiene por incidente, y a partir de una estimación de incidentes por año, nos permitiera decidir sobre la estrategia que hay que implantar (aceptar el riesgo tal como es y definir un plan de contingencia en caso de producirse, o bien mitigarlo mediante desarrollos adicionales, otras herramientas o cambios en el diseño que lo permitan).

- Sin entrar en detalle, enunciamos a continuación un conjunto de buenas prácticas genéricas que ayudarán a mitigar los riesgos asociados a cualquier proyecto:
- Asignar el mínimo privilegio posible a cada actor en el sistema.
- Simplicidad. La seguridad por ofuscación no da buenos resultados.
- Diseño abierto. Siempre tendremos alternativas para mejorar o asegurar más el sistema.

- Seguridad por defecto. El sistema debe ser el máximo de seguro por defecto, si tiene que ser posible relajar las restricciones, debe tratarse de una acción adicional a realizar con el proyecto ya implantado.
- Fallada segura. Si el sistema falla o puede fallar, evitar que lo haga quedándose en una modalidad insegura.
- Minimizar el uso de recursos compartidos.

Trabajar a favor de la usabilidad del proyecto redunda en un mejor uso de él y en menores probabilidades de fallos de seguridad por un mal uso del mismo.

ANEXO B
ESTÁNDARES

B.1 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.

ANEXO C
SISTEMAS DE VOTACIÓN VERIFICABLES DE EXTREMO A EXTREMO (E2E)

El desarrollo de los sistemas de votación verificables de extremo a extremo se produjo como una solución frente a la necesidad mantener el anonimato y asegurar la fiabilidad de los protocolos de votación. Siguiendo el trabajo de Panizo Alonso (PANIZO ALONSO, 2014), los sistemas de votación verificables de extremo a extremo (E2E) (End-to-End auditable voting systems) se caracterizan por su importante integridad y seguridad ante los intentos de adulterar el voto.

Los sistemas (E2E), emplean métodos de cifrado complejos para elaborar comprobantes que permitan a los votantes verificar que sus votos han sido contabilizados correctamente sin poner en peligro el secreto del voto. Por esta razón, en algunas ocasiones, son denominados sistemas basados en recibos (receipt-based systems) (FINK, 2010).

A continuación, se presentan algunos de los sistemas de votación verificables de extremo a extremo.

El primer intento es realizado por David Chaum en 1981 (CHAUM, 1981) en el que se propone un proceso electoral donde cualquier persona pueda verificar, que los votos han sido contados correctamente mediante una firma anónima del voto antes de ser enviado por correo electrónico. Esta solución está basada en criptografía de clave pública y permite ocultar al votante, así como el contenido de su

voto, a pesar de utilizar una infraestructura de comunicación como Internet. La técnica dispone de un protocolo que comprueba que el voto proviene de un elector legítimo.

Las soluciones para ser utilizadas sobre Internet fueron desarrolladas en principio en la tesis de Ben Adida en el 2006, dirigida por Ronald Rivest (ADIDA, 2006) y posteriormente con las tesis doctorales de Richard Carback y Russell Fink en el 2010, dirigidas por Alan Sherman (FINK, 2010) (CARBACK III, 2010).

De acuerdo con la EAC (UNITED STATES ELECTION ASSISTANCE COMMISSION, 2005) las características, que distinguen los sistemas E2E, son las siguientes:

- Cada votante obtiene un recibo en papel que contiene la información necesaria para poder verificar que su voto ha sido grabado correctamente y que esta información no permita revelar a terceros lo que se ha votado.
- El votante tiene la posibilidad de comprobar que su voto ha sido contabilizado. Esta operación puede realizarse por diversos medios, como por ejemplo a través de un sitio web en el que deberá coincidir la información impresa en el recibo con la expuesta en el mismo.

Tales sistemas no solamente deben garantizar que el voto ha sido correctamente grabado, es decir tal y como fue emitido, sino que fue contabilizado de la misma forma.

Vemos, que debido a la importancia, que tiene en las elecciones democráticas, el secreto del voto, los sistemas E2E deben cumplir con el hecho que el recibo entregado

al votante, no permita identificarlo, ya que esta situación vulneraría el secreto del voto. Siendo estos sistemas los más avanzados tecnológicamente es necesario evaluarlos y compararlos para disipar dudas sobre sus aspectos legales, administrativos o sociales y clasificarlos en función de cómo cumplen, con los aspectos más importantes de una votación democrática.

En los sistemas de votación electrónicos más modernos utilizados en la actualidad, es necesario que una máquina imprima recibos a los votantes posteriormente a la votación. Este método permite asegurar al votante que su voto es contabilizado de forma correcta y de acuerdo a la elección que haya realizado.

Los sistemas de votación (E2E), se basan en criptografía para lograr la verificabilidad de extremo a extremo, ofreciendo la posibilidad de que cualquier votante sea capaz de auditar el proceso de votación por completo y realizar la trazabilidad de su propio voto. Pero, como se dijo al mismo tiempo, estos sistemas en sus procesos de revisión deberían garantizar la necesidad de mantener el secreto del voto para evitar la coacción sobre el votante. Sin embargo algunos sistemas basados en la emisión de un recibo en papel no proporcionan seguridad sobre el secreto del voto, ya que el número único que aparece impreso en el voto, puede ser rastreable hasta el nombre del votante. Por este motivo, la mayor parte de los desarrolladores de (E2E) usan técnicas criptográficas para mantener la identidad del votante en secreto y asegurar que todos los votos emitidos son legítimos.

- Existen distintos desarrollos de sistemas E2E, como ser:
- **Helios**. Es un desarrollo en código abierto y público que permite generar un proceso de votación remota basado en web. Desarrollado por Ben Adida y su equipo en el 2006. Está basado en un protocolo verificable y sencillo propuesto por Benaloh (BENALOH, 2006) y ha sido utilizado en varias ocasiones, ya que permite un uso público y sencillo.
- **Adder**. Es una propuesta muy similar a la anterior con la que tiene varios aspectos en común: código abierto y público y posibilidad de verificación por parte del votante. Fue desarrollado por el Departamento de Ingeniería y Ciencias de la Computación de la Universidad de Connecticut por Aggelos Kiayias y su equipo en el 2006 (ADDER, 2014). Utiliza criptografía homomórfica (KIAYIAS, 2006), pero el proyecto ha sufrido una parada en 2009.

Votehere, **Scytl Pnyx** y **SureVote** son implementaciones comerciales en las mismas fechas que las anteriores. En este caso están protegidas por patentes.

- A continuación analizaremos algunos sistemas que proporcionan mecanismos de verificación E2E y son de tipo presencial:
- PunchScan de David Chaum (2005) (ESSEX, 2014)
- Scantegrity de David Chaum (CHAUM, 2008)
- ThreeBallot de Ronald Rivest (RIVEST, 2006) (RIVEST, 2007)
- Scratch&Vote de Ben Adida y Ronald Rivest . (ADIDA Y RIVEST, 2006)

- Prêt à Voter de Peter Ryan (RYAN, 2007) (RYAN, 2009) Bingo Voting de Bohli/Müller/Röhrich (BOHLI, 2007)

C.1.- PUNCHSCAN

Este sistema fue propuesto originalmente por David Chaum y desarrollado en código abierto (licencia BSD) en diciembre de 2005, actualmente el proyecto está integrado en su sucesor, el Scantegrity (CHAUM, 2006). Previamente este autor propuso en 1981 el concepto de votación electrónica verificable y una primera propuesta de sistema de votación electrónica utilizando cifrado visual en 2004 denominado Votegrity (CHAUM, 2004). Desde el 2011 el Punchscan ha desaparecido como tal e incluso el portal de descargas de su código ha sido eliminado, pasando oficialmente a ser una parte del Scantegrity.

Esta solución fue presentada al concurso VoComp organizado en 2007 para comparar diversos proyectos de voto electrónico quedando en primera posición. Para ello tuvo que demostrar sus ventajas sobre otras propuestas y entregar un documento riguroso describiendo el sistema, sus especificaciones, el código fuente (abierto), el análisis de seguridad y su autoevaluación. Además ha sido utilizada en las elecciones de la asociación de estudiantes de la Universidad de Ottawa (marzo 2007) y en una encuesta sobre privacidad, libertades y computadores desarrollada en Montreal en mayo de 2007.

Las ideas básicas de esta solución son aportar una auditoría pública pre y post electoral y que el votante obtenga un recibo de votación. La verificación puede ser

realizada por el propio votante, las autoridades electorales y por observadores independientes. Esta comprobación intenta demostrar que el voto ha sido contabilizado como fue emitido y que este recuento se ha desarrollado correctamente y preservando el secreto del voto.

La verificación se puede llevar a cabo sobre todos los votos, por cualquiera, sobre el software y el hardware independiente y utilizando el código abierto.

Como condición necesaria aparece la imposición de que cada boleta sea única y para ello muestra un número de serie y un diseño irrepetible, lo que sin duda complica su impresión. Con ello se intentan conseguir dos propiedades, la integridad del sistema y el secreto del voto. Otra característica esencial es el hecho de que se generen el doble de las boletas necesarias para el proceso electoral, con el fin de poder llevar a cabo un proceso de verificación antes del comienzo del proceso de votación.

El método se basa en un recuento óptico de los votos. El votante marca su elección sobre un papel pre-impreso con dos hojas adosadas y no sobre una pantalla. Posteriormente, parte de la boleta queda en poder del votante, después de ser escaneada, a modo de recibo para ser utilizada en la verificación posterior. El secreto del voto no se ve comprometido ya que no se puede volver a reconstruir sin la información que sólo está en poder de las autoridades electorales. Gracias a esa información, que siempre permanece en privado, se puede realizar el recuento pero también es posible publicar los datos necesarios para que el votante pueda verificar que su voto ha sido contabilizado correctamente sin desvelar su elec-

ción. En principio este esquema está dentro de los parámetros propios de un método de votación que cumple con los criterios básicos de unas elecciones democráticas y añade la posibilidad de una verificación tipo E2E (POPOVENIUC Y HOSP, 2010), (POPOVENIUC Y HOSP, 2014).

Como descripción básica, el voto tiene dos capas de papel. En la superior, se ven los candidatos con un símbolo o letra al lado de su nombre y a continuación hay una serie de agujeros redondos en la capa superior de la boleta. Dentro de estos agujeros y en la capa inferior están impresos los símbolos correspondientes a cada candidato pero no relacionados con el nombre del mismo. Ambas hojas tienen el mismo número de serie. El votante dispone de un rotulador de punta gruesa con el que marca su elección, señalando con tinta tanto en la hoja inferior como en la superior. Inmediatamente después se separan las hojas y se destruye mediante una destructora de papel una de ellas en público y de forma aleatoria.

El procedimiento de votación requiere una formación previa del votante y de los miembros de la mesa, disponer de las boletas y de un soporte similar a una carpeta con una pinza que sujeta las dos hojas de la boleta. En la zona de votación no se accede directamente a las boletas sino que son entregadas por el personal de la mesa una vez que el votante ha sido identificado y al mismo tiempo se le indica, de forma aleatoria, la parte de la boleta que ha de destruir posteriormente.

La boleta es leída con el equipo de escaneado óptico (OCR) que dispone la mesa y al mismo tiempo sale una

copia por la impresora, que está conectada al mismo, y que será entregada a modo de recibo al votante, verificándose la coincidencia con el original que queda en la urna electoral. Cada par de boletas tiene un número de serie único, que podría ser vinculado al votante pero no a su elección ya que la posición de los candidatos no es descubierta en ningún momento y se utilizará en el posterior proceso de verificación que asegura que el voto ha sido contabilizado. Después del recuento, la autoridad electoral publicará una imagen de cada recibo a través de una web. El votante puede buscar su voto escribiendo el número de serie y puede comprobar que la información en poder de la autoridad electoral coincide con su voto. De esta manera, el ciudadano puede estar seguro de que su voto fue tenido en cuenta como estaba previsto.

Cualquier elector o parte interesada puede también inspeccionar parte de los registros de los votos para verificar que los resultados se calculan correctamente, pero no pueden revisar toda la base de datos, ya que de lo contrario se podrían vincular votos a números de serie. Sin embargo, los autores aseguran que se puede inspeccionar la mitad de la base de datos sin romper el anonimato. Se demuestra con este procedimiento que la probabilidad de que todos los votos fueron contabilizados adecuadamente es muy alta (FISHER, 2006).

El orden de los símbolos y de los nombres que aparecen en las boletas son generados seudo-aleatoriamente para cada votación y por lo tanto difiere en cada una de ellas. Del mismo modo ocurre con el orden de los símbolos en los agujeros. Por esta razón, el recibo no contiene

suficiente información como para determinar qué candidato fue elegido. Si se mantiene la capa superior, el orden de los símbolos a través de los agujeros es desconocido y si se mantiene la inferior, el orden de los símbolos al lado de los nombres de los candidatos también es desconocido. Por lo tanto el votante no puede demostrar a nadie cómo ha votado, lo que impide la compra de votos o la coacción a los votantes. Por otra parte a cada boleta se le asigna un número de serie. La relación entre el número de serie y el tipo de boleta solo se establece en el momento del recuento, mediante la introducción de las claves en poder de las autoridades electorales.

El sistema dispone de un algoritmo mediante el cual puede recuperar la información de la hoja que ha sido destruida, a partir del número de serie y con total seguridad.

Si durante el proceso electoral fallara algún dispositivo electrónico, las elecciones podrían continuar si se toman los datos de forma manual y reteniendo la parte de la boleta que habría que destruir, pero esto complicaría aún más el proceso.

La integridad y verificabilidad de los resultados es el aspecto más fuerte de este sistema. Es muy importante la posibilidad de comprobar el código de la aplicación al ser abierto y las primitivas de seguridad empleadas para proteger la información son consideradas hoy en día suficientemente robustas (AES y SHA-256) aunque mejorables.

El sistema cumple en lo esencial con las comprobaciones posibles, tanto la que puede llevar a cabo el elector para comprobar que su voto ha sido tenido en cuenta de

la misma forma en que fue emitido y la general que pueden llevar a cabo las autoridades electorales.

Punchscan fue un sistema pionero de votación con verificación E2E aunque con documentación poco clara y detallada. El equipo que lo desarrolló ha sido capaz de innovar para cumplir con los requisitos que les impusieron en cada elección o prueba hasta el 2008. A partir del 2011 el sistema desapareció y con él el código abierto. En este momento este proyecto fue integrado en el sistema Scantegrity.

C.2.- SCANTEGRITY

Es una variante de la anterior propuesta por el mismo autor, David Chaum, con la colaboración de otros investigadores como Ronald Rivest y Peter Ryan. El proyecto ha sido mejorado por propuestas de los mismos autores, como el Scantegrity II. (CHAUM, 2008), o por terceros como el caso del Scantegrity III (SHERMAN, 2011).

Esta propuesta ha sido utilizada en diversas ocasiones lo que ha conseguido mejorar y refinar su diseño. La primera ocasión fue el 9 de noviembre de 2007 en la conferencia "Claim Democracy" en su versión inicial. Posteriormente, en 2008, las experiencias se desarrollaron con Scantegrity II en diversas consultas populares en Ottawa (grupo de usuarios de Linux) y en Takoma Park (CARBACK, 2010). La más singular e importante se desarrolló el 3 de noviembre de 2009 (SHERMAN, 2011) en las elecciones municipales de esta última localidad americana. A raíz de esta votación se propusieron diversas mejoras que concluyeron con la propuesta del Scantegri-

ty III, pero que no ha llegado a ser utilizada en ningún proceso electoral.

En este caso la votación se realiza mediante una lectura óptica de la boleta mediante un OCR y manteniendo al mismo tiempo las boletas originales para que puedan ser analizadas de nuevo manualmente si fuera necesario. A diferencia del caso anterior, este sistema puede ser utilizado en cualquier proceso que utilice un escáner óptico convencional y se desarrolla como un proceso de votación muy similar al clásico, en el que no hay que añadir ningún equipamiento adicional, salvo una impresora para imprimir información adicional sobre la boleta en el momento de la impresión.

En la segunda variante, Scantegrity II, se utiliza papel especial que oculta códigos de confirmación de la selección que sólo son visibles cuando son marcados con una tinta especial, lo que sin duda mejora el principal inconveniente de la anterior versión que era la resolución de las impugnaciones.

Sobre la base del Punchscan, es decir sobre un sistema de votación basado en el escaneo óptico del voto, se optó por integrar un proceso seguro de verificación, lo que obligó a un diseño nuevo y específico de la boleta y a modificar el procedimiento de votación. En principio el Scantegrity sólo necesita que se imprima en las boletas una información adicional que no aparecía en el Punchscan. Como se quiere que las boletas sean únicas, es esencial desligar la boleta del votante. Para ello se utiliza la sencilla solución de dividir la boleta en dos en el

momento de depositar el voto, no existiendo mecanismo que pueda unirlas salvo bajo la supervisión de las autoridades electorales y sólo para el recuento.

En esta solución, al igual que en otras, parte de los votos, típicamente la mitad, son elegidos al azar antes de las elecciones para realizar una verificación pública y demostrar que la propuesta es fiable. Lo más complejo es revelar la suficiente información para verificar el voto sin comprometer el secreto del mismo. Otro aspecto delicado es resolver las impugnaciones entre el votante y las autoridades electorales cuando el primero asegure que su voto no ha sido contabilizado correctamente.

En la primera versión del Scantegrity el procedimiento era similar al utilizado en cualquier votación con escáner óptico, en el que el elector deposita la boleta en la urna que es leída por el OCR, salvo que el votante se llevaba a casa un recibo de su voto. Por tanto éste recogía la boleta, en la que la relación entre los candidatos y las letras que tiene que marcar el votante no son únicas, y señala con un rotulador especial su elección para a continuación entregar su voto en la urna con lectura óptica. La única diferencia que aprecia el votante con respecto al voto clásico en urna con lector óptico, es que puede arrancar parte de la boleta que contiene un número de serie y su codificación en código de barras y en la que puede anotar la letra asociada al candidato elegido. Después del recuento se publican los números de serie y la letra asociada a cada uno de ellos sin desvelar el nombre del candidato. De esta forma el elector puede verificar

que su voto ha sido correctamente explorado y registrado pero no puede demostrar a un tercero a quién votó. El problema aparece cuando el votante discrepa de la opción por la que ha votado y desafía al sistema impugnando la votación.

En este caso el procedimiento para resolver la impugnación tiene dos pasos. En primer lugar los miembros de la mesa tienen que recuperar la boleta original leída por el escáner óptico para verificar el número de serie pero no su contenido, algo que evidentemente ha de hacerse con las suficientes garantías. En segundo lugar ha de comprobarse la opción marcada sin comprometer al candidato seleccionado leyendo el número de serie y buscando la coincidencia con el listado publicado después del recuento. Si esta no se produce, es suficiente para que la impugnación prospere y se modifique el recuento. Todo esto evidenció la débil estructura de resolución de conflictos y propició la aparición del Scantegrity II (Invisible Ink).

En esta versión no existe relación directa entre el número de serie de la boleta utilizada y la posición de las marcas sobre la misma, ya que esto se resuelve utilizando unos rotuladores que descubren, mediante tinta especial, unos números ocultos que además permiten la resolución de impugnaciones de una forma que los autores defienden como más sencilla y transparente.

El procedimiento de votación con Scantegrity II es muy similar al de un sistema de votación con escáner óptico, excepto que la casilla en la que se señala la elección

contiene un código de confirmación impreso al azar y en tinta invisible. El votante marca la casilla elegida con un bolígrafo “decodificador” diseñado al efecto, que activa la tinta invisible provocando que aparezca un código de confirmación. Esta es una diferencia esencial con la primera versión.

Los electores que deseen comprobar su voto posteriormente pueden anotar los códigos de confirmación en un cupón recortable que contiene el número de serie de la boleta, o bien pueden sencillamente ignorar el código y emitir su voto con normalidad.

Los códigos de confirmación se asignan aleatoriamente en las boletas de voto por lo que los votantes pueden compartir libremente sus códigos manteniendo en secreto su voto, aunque no le conste fehacientemente que su código corresponda a su elección en el momento del recuento.

Una vez finalizada la votación, la autoridad electoral publica una lista con los códigos de confirmación seleccionados en cada boleta sin precisar la posición, con lo que no se compromete el secreto del voto y se evita la coacción. Los votantes que copiaron sus códigos pueden verificar que se han tenido en cuenta en el escrutinio y que no se han quitado ni añadido otras opciones.

Después del recuento, los administradores electorales generan una lista por número de serie con las boletas y sus códigos de confirmación. Dado que el vínculo entre el código de confirmación y el candidato votado permanece en secreto, el recuento se realiza utilizando un proceso

que garantiza la preservación del anonimato. El recuento puede ser comprobado por cualquiera para asegurar su precisión (verificación universal).

La seguridad del sistema no requiere de ningún software específico para funcionar correctamente, sólo necesita que las operaciones matemáticas (que no son públicas) sean confirmadas de forma independiente por todas las partes interesadas, sobre todo en lo que se refiere a la generación aleatoria de los números de serie de las boletas y a los códigos de elección.

El Scantegrity II mejora la integridad del sistema original dado que evita la coerción directa aun disponiendo de acceso a las boletas ya que los códigos están ocultos y la única forma de acceder a ellos es invalidar la votación. Obviamente la parte de la boleta depositada en la urna contiene ambas informaciones, es decir el número de serie y el código con la elección, por lo que el acceso a las mismas está restringido a los miembros de la mesa y sólo si fuera necesario acceder a ellas.

Para la impresión de las boletas se utilizan tres tipos de tintas diferentes: una es tinta convencional para la impresión de los datos básicos de la votación más los nombres de los candidatos; las otras dos tienen que ver con los códigos de confirmación y con el sistema de lectura óptico. Las interacciones entre éstas y el producto químico que las activa, presente en el rotulador utilizado para marcar el voto, no son sencillas y constituyen una fuente de problemas adicionales en este tipo de sistemas.

Las pruebas reales realizadas con este sistema, dejaron patente que algunos votantes no escribían los códigos de verificación para poder posteriormente realizar la comprobación sobre su voto y que el votante no era informado con claridad de cuántas opciones disponía al votar por lo que podía hacerlo de forma incorrecta.

En Scantegrity III, tercera variante, propuesta por Sherman (SHERMAN, 2011) se definen mejoras obtenidas mediante observación en una elección real en noviembre del 2009. La más destacada se refiere a la impresión automática del recibo de verificación, lo que reduce la instrucción previa del votante y por tanto mejora la usabilidad, incrementa la accesibilidad, facilita la detección por parte del votante de la manipulación de su voto y hace más sencilla la verificación posterior.

Una vez que la boleta es marcada por el votante, se coloca debajo de una tapa de cristal donde es explorada ópticamente y los detalles más importantes, letra, nombre y código de la opción elegida, son destacados con una luz trasera. Posteriormente se visualizan los dos formatos disponibles de recibo de verificación para de forma aleatoria imprimir uno de ellos. Este mecanismo de impresión reduce los riesgos en esta parte del proceso. Esto permite simplificar el proceso y mejorar aspectos como la notificación al usuario de haber rellenado correctamente la boleta y reducir la posibilidad de que la misma sea modificada posteriormente añadiendo marcas después de contabilizada, que podrían llevar a la impugnación del proceso.

Esta versión intenta aumentar la usabilidad del sistema mediante la retro-iluminación de la boleta en el momento de la lectura óptica, destacando los aspectos básicos del voto. Para cumplir con estos aspectos aparece un nuevo dispositivo, denominado PCOS, que integra el escáner óptico con retro-iluminación, el detector de las marcas en las boletas y la impresora que entrega el recibo de votación en uno de los dos formatos definidos.

Este sistema utiliza un generador de números seudo-aleatorios (PRNG) como en el caso anterior pero utiliza cuatro tablas para realizar las operaciones de mezcla (mixnets). Estas tablas se denominan P, Q, R y S. La tabla P relaciona los códigos de confirmación y los candidatos en cada boleta, se genera bajo la supervisión de las autoridades electorales y nadie debería de tener acceso a ella, pero se utiliza para generar la tabla Q. En ésta se publican los códigos de confirmación pero realizando una permutación seudo-aleatoria de forma que cada fila i corresponda a la boleta i pero en cada columna no hay correspondencia con candidatos fijos. De esta tabla Q sólo se publican los códigos de confirmación utilizados. En la tabla R se desarrollan dos mezclas al azar de los códigos de confirmación y será utilizada en el procedim

C.3.- THREEBALLOT

ThreeBallot es un protocolo de votación desarrollado en el 2006 por Ronald Rivest (RIVEST, 2006). Es un sistema que puede ser implementado en papel convencional. El objetivo de su desarrollo es obtener un diseño

sencillo, de fácil comprensión y que no utilice técnicas de cifrado complejas.

Ha sido utilizado en una votación en diciembre de 2006 por estudiantes del M.I.T. que dejaron en claro problemas de privacidad, seguridad y usabilidad.(CALIFORNIA INSTITUTE OF TECHNOLOGY, 2014). En ella el 20% de los votantes consiguieron vender sus votos, el 10% no fue capaz de verificarlo y el 30% no consiguió emitir correctamente el voto en el primer intento.

ThreeBallot intenta resolver el problema de la contraposición entre verificabilidad y anonimato dando a cada votante tres boletas. De una de ellas se hará una copia y servirá de recibo y las tres se depositarán por separado en la urna. Cada boleta de las tres tiene un número único y distinto, intentando evitar que el número sea excesivamente grande con objeto de que sea más sencilla su gestión. El votante elige qué boleta va a ser su recibo para verificar la votación. El que recuenta los votos obviamente no lo sabe y tiene una probabilidad de 1/3 de ser descubierto destruyendo o alterando el voto. El elector vota por una opción (sí/no) o candidato en cada fila de forma que está obligado a marcar un par de veces para que sea válida, ya que una marca no es suficiente por razones que veremos a continuación. De esta forma el recuento sólo es válido si tiene dos marcas en cada fila, que corresponden a un candidato o pregunta. Por ello para votar por un candidato el elector debe seleccionarlo en dos de las tres partes de la boleta.

Para votar en contra de un candidato (el equivalente a dejar un voto en blanco en otros sistemas), el votante debe seleccionar a ese candidato solamente en una boleta. Ningún candidato puede dejarse en blanco, ni se puede seleccionar en las tres boletas. El recibo con el que se queda el votante, es decir una copia de una de las tres partes de la boleta, no puede demostrar a un tercero a quién se ha votado, con lo que se evita la compra de votos y la coacción sobre el votante. Todos los votos emitidos son escaneados y publicados después del recuento para proporcionar un procedimiento de verificación y para detectar manipulaciones en los votos depositados. Es imposible relacionar las tres partes de la boleta y sus números de serie son aleatorios y únicos.

Resumiendo, en primer lugar el votante selecciona aleatoriamente una de estas boletas triples. A continuación marca su elección por filas de tal forma que no puede dejar ninguna fila en blanco y al menos ha de poner una marca por fila, ya que de otra forma el voto no será válido y detectado como tal en el momento de la emisión. Si el votante desea NO VOTAR por un determinado candidato tiene que realizar UNA marca en la fila correspondiente en cualquier posición (columna). Si el votante desea VOTAR a favor de un candidato necesita poner DOS marcas en esa fila y en cualquiera de las tres columnas de la boleta. En ningún caso debe marcar TRES ya que el voto también sería nulo y no sería admitido en la urna.

Antes de depositar la boleta es necesario verificar la validez del voto y esto tiene que realizarse en un equipo

que explore ópticamente el voto y detecte los nulos impidiendo la emisión del mismo. Obviamente este sistema no puede estar conectado a nada ni tener capacidad de almacenar información, lo cual puede no resultar obvio.

Una vez verificada la validez de la boleta, el proceso de votación se desarrollará de la siguiente forma: se procederá a separar las tres partes de la boleta en presencia de la mesa pero sin mostrar las opciones marcadas, se realizará la copia en privado pero bajo la supervisión de los miembros de la mesa, de una de las tres partes de la boleta que el votante elegirá libremente y que mantendrá como recibo para la verificación posterior y por último, las tres boletas originales se dejan caer en la urna por separado. La copia que ha de ser realizada bajo la supervisión de los miembros de la mesa es para evitar que el votante haga una copia de toda la boleta.

Al final de la votación todas las boletas se publican, mediante un sitio web que hará las veces de tablón de anuncios y en el que cada elector puede verificar que sus votos fueron contabilizados buscando el número de su recibo (copia de boleta elegida) entre los números de las boletas publicadas. Sin embargo, con el recibo del elector no se puede deducir cuál ha sido su voto válido ya que ha podido quedarse con cualquiera de las boletas, por lo que no puede demostrar a un tercero el sentido de su voto eliminando la posibilidad de coacción. También existe la posibilidad de impugnar la votación en el caso de que el recibo no aparezca o no coincida con el publicado, lo que podría poner en jaque todo el proceso electoral. Si el número de

triples boletas contabilizadas coincide con el número de votos emitidos podemos estar seguros que no se han añadido durante el proceso.

El principio clave de este sistema se basa en considerar cada voto como una matriz, en la que las filas corresponden a cada candidato o pregunta y en las que el votante se debe fijar para expresar su elección (votar por filas), pero el procesamiento del voto se hace depositando en la urna las tres partes de la boleta por separado, siendo recontadas por el sistema (procesado por columnas).

Si la boleta está correctamente diseñada, disponiendo dos líneas micro-perforadas que permitan la separación limpia de las tres partes, una zona para marcar la opciones diseñada para permitir la lectura automatizada por parte de un escáner óptico y los números de serie de cada una de las tres partes de la misma impreso en código de barras, posibilitaría una lectura simple y rápida de cada voto. Con ello sería rápido y fiable el recuento y la publicación de todos los votos.

En cuanto al recuento cada candidato o pregunta tiene de partida un voto por cada votante ya que al menos una de las tres boletas ha de ser marcada. Pero adicionalmente aquellas que han sido seleccionadas por el votante han recibido una marca más, que es la que realmente tiene que contabilizarse.

El sistema se basa en que la autoridad electoral tiene que disponer de los números de serie de las tres boletas que integran cada voto para poder imprimir las boletas y resolver las impugnaciones.

ThreeBallot logra que los votantes puedan verificar su voto y mantener el anonimato, no teniendo que utilizar sofisticados procedimientos basándose en terceros de confianza, ni protocolos que impidan la trazabilidad del voto. El esquema es de gran importancia teórica, ya que demuestra que es posible diseñar una solución verificable (E2E) sin apenas uso de la criptografía.

Posteriormente el autor ha mejorado su propuesta inicial modificaciones, denominadas VAV y Twin, que permiten reducir las vulnerabilidades y aumentar la usabilidad del sistema (RIVEST Y W. D. SMITH, 2007)

C.4.- SCRATCH&VOTE

Esta propuesta del 2006, surgió de la tesis doctoral de Ben Adida dirigida por Ronald Rivest (ADIDA, 2006). Al mismo tiempo se publicó un artículo científico firmado por ambos (ADIDA Y R. L. RIVEST, 2006). Este desarrollo es una propuesta académica que no ha sido puesta a prueba.

El sistema Scratch&Vote permite a los votantes comprobar que sus votos han sido procesados correctamente sin necesidad de apoyo por parte de las autoridades electorales. Además esta solución, según descripción de sus desarrolladores, ha sido diseñada para minimizar el coste y aumentar la usabilidad incidiendo en tres aspectos: los votos son en papel y se pueden imprimir utilizando tecnología convencional, son verificables universalmente y además el recuento sólo requiere de un descifrado sencillo, basado en la confianza de las partes. En suma

la verificación del proceso por parte del votante puede realizarse incluso antes de emitir su voto.

Esta solución combina propuestas de trabajos anteriores como la posibilidad de seleccionar múltiples candidatos de (Baudron BAUDRON, 2001), la sencillez de la boleta de Chaum (CHAUM, 2004) y las técnicas avanzadas de Ryan (RYAN, 2007). La gran diferencia está en el uso de contadores con cifrado homomórfico para el recuento de los votos, en vez de las *mixnets,* por lo que la implicación de la autoridad electoral se limita al descifrado de un sencillo texto cifrado por cada vuelta.

Scratch&Vote hace que el proceso de verificación por parte del votante sea seguro porque permite que un voto de papel sea revisado sin tener que involucrar a nadie más. Este método introduce la novedad de una superficie de rascado en la parte inferior de la zona en la que aparecen los nombres de los candidatos. El orden en el que aparecen impresos estos nombres se oculta debajo de esta superficie de rascado y cifrado. Para comprobar que un voto no está alterado, el votante simplemente tiene que rascar la superficie correspondiente para ver el número oculto que guarda una correspondencia con el orden de los nombres de los candidatos. En teoría, los autores dicen que los votantes podrían usar el software criptográfico en la sede electoral o por Internet para verificar este orden, pero proporcionen los medios necesarios para verificarlo. Si el código que posee el elector coincide con el publicado en el *bulletin board*, entonces el voto revisado es legítimo y por tanto habría sido correctamente contabilizado.

La diferencia fundamental está en el uso del cifrado homomórfico que garantiza la imposibilidad de conocer la identidad del votante, pero sí el recuento preciso.

El votante recibe dos boletas que a simple vista sólo se diferencian en el orden en el que se muestran los candidatos y decide qué boleta es la que va a verificar y cuál la que va a utilizar para votar. En la primera "rasca" la superficie dispuesta para ello permitiendo que aparezcan unos dígitos que indican el orden de cada candidato, con los cuales y por medio de una aplicación de descifrado y utilizando una clave pública podrá comprobar que el orden de los candidatos coincide con el impreso en la boleta y con el descrito en el código de barras, que está cifrado con una clave privada que sólo conoce mancomunadamente la mesa electoral. Esto lo puede realizar incluso antes de votar. Después marcará su elección en la otra boleta y recortará la zona de la izquierda en la que figuran los nombres de los candidatos, con lo que se garantiza el anonimato. Después se acercará a la mesa de votación y el presidente de la misma comprobará que la superficie de rascado está intacta para evitar la venta de votos y separará esta parte de la boleta para destruirla inmediatamente evitando que alguien pueda comprometer el secreto del voto. A continuación y mediante escáner óptico se leerá la posición de la marca y el código de barras que cuando se cierre la urna serán publicados con el fin de que el votante pueda comprobar que su voto ha sido tenido en cuenta. Esta información queda protegida dentro de la urna para evitar perder el secreto del voto. Por último el votante se lleva a modo de recibo esta mis-

ma parte de la boleta que utilizará para verificar su voto posteriormente.

Para realizar el escrutinio la urna reconoce la posición de las marcas y mediante el código de barras y el algoritmo de descifrado basado en clave privada presente en el equipo y bajo autorización de los integrantes de la mesa, realiza la contabilidad de los votos. También se pone en el "tablón de anuncios" ya sea en el local o a través de Internet, toda la relación de votos emitidos en la urna, con lo que el votante podrá verificar que el suyo ha sido contabilizado.

El uso del homomorfismo en los procesos electorales fue propuesto por Baudron (BAUDRON, 2001) con objeto de garantizar el anonimato en el recuento de los votos de estructura múltiple debido a que un observador externo no puede sacar conclusiones observando las operaciones homomóficas que se realizan sobre los votos que en ningún caso son descifrados.

Inicialmente se utiliza el cifrado con clave pública de Paillier (PAILLIER, 1999) que proporciona un cifrado semántico seguro con la característica de disponer de homomorfismo en las operaciones de adición. Para ello se utilizan contadores homomórficos descritos por Baudron que funcionan de tal forma que un observador externo no puede decir qué contador interno ha sido incrementado al recibir el voto pero sí que ha sido tenido en cuenta. En otras palabras, la suma homomórfica utilizada por este sistema puede ser verificada por cualquiera sin desvelar el secreto de anonimato.

El aspecto fundamental de este sistema está en que los parámetros básicos de las elecciones se publican previamente, indicando el orden de los candidatos, es decir asignando un número a cada uno de ellos, además de la clave pública y M que es la longitud en bits necesaria para representar los valores de los contadores de cada candidato. En la propia boleta, además del nombre de los candidatos y el espacio a la derecha correspondiente para realizar la marca de selección, está ubicado el código de barras que contiene la información cifrada con la clave pública de la posición de los nombres (r_1,r_2,r_3,r_4) y finalmente y en la parte inferior, una zona que se recorta antes de depositar el voto con la posición de los candidatos en la boleta, que puede ser utilizada para la verificación de la misma antes de la votación, siendo en este caso la boleta inválida para votar ya que podríamos conocer a quién ha votado el elector.

Una vez cerrado el proceso de votación, es suficiente para realizar el recuento del voto la interacción entre la información pública del proceso, la posición de la marca y la información cifrada en el código de barras, para supuestamente conseguir un recuento seguro y transparente sin relación ninguna con el votante.

Los datos publicados deben estar certificados por algún mecanismo como firmas digitales que garanticen que son los correctos.

Esta solución está basada en un complejo soporte criptográfico, cuyos detalles sólo están al alcance de ver-

daderos expertos. No existen pruebas reales por lo que se desconocen sus resultados prácticos.

C.5.- PRÊT À VOTER

Este esquema fue propuesto por Peter Ryan de la Universidad de Luxemburgo entre el 2004 y el 2006 y lo denominó Prêt à Voter (PRÊT À VOTER, 2005) (RYAN, BISMARK,)pero la idea inicial fue propuesta en colaboración con David Chaum (CHAUM, 2005). Posteriormente se desarrolló una implementación para un concurso-votación en el 2007 (BISMARK, 2009) en el que quedó en segundo lugar después de PunchScan pero ganó en el apartado de mejor diseño. Actualmente el proyecto sigue vivo bajo la denominación *Trustworthy Voting Systems* (TRUSTWORTHY VOTING SYSTEMS, 2013) con el trabajo de dos grupos de investigadores de las Universidades de Surrey y Birmingham y el apoyo de la de Luxemburgo.

En esencia es un sistema de votación que utiliza escaneo óptico del voto y un modelo criptográfico basado en *mixnets.* Se fundamenta en que en una mitad del voto aparecen los nombres de los candidatos en un orden aleatorio que es destruida antes de votar y en la otra mitad aparecen las casillas de selección para que el votante señale el candidato que desee. Esta última mitad contiene un número de serie que permite bajo circunstancias controladas averiguar a qué candidato se ha votado y le sirve al votante como recibo de verificación.

En su desarrollo práctico se ha utilizado para una votación de estudiantes en un entorno de concurso denominado VoComp que se realizó en julio de 2007 en Ore-

gon (VOCOMP, 2009); También fue probado en la Universidad de Newcastle en mayo del 2007 con la intención de mejorar su usabilidad y fiabilidad (WINCKLER, 2009) .

En este sistema el votante, antes de proceder a emitir el voto, retira la columna de la izquierda de la boleta con el nombre de los candidatos y la destruye en presencia de los miembros de la mesa para preservar el secreto del voto. A continuación el votante se dirige a la urna que en realidad dispone de un escáner óptico, el cual lee el voto con la marca de selección y el número de serie único que figura en la parte inferior de la boleta, que servirá posteriormente para recuperar mediante una clave secreta el orden de los candidatos en esa boleta y también para poder verificar que el voto ha sido correctamente contabilizado mediante un tablón de anuncios (*bulletin board)* en el que se publican todos los votos emitidos con su número de serie. Después de que el voto sea leído se procede a firmar digitalmente el archivo escaneado, por parte de la mesa electoral, y el votante se queda con esta mitad del voto que no contiene los nombres de los candidatos de las casillas de selección.

Existen dos mecanismos para verificar los votos. Por una parte cada votante puede comprobar que su voto ha sido tenido en cuenta comparando su recibo con el listado de los votos emitidos que se publican en el tablón de anuncios, mediante el cual verifica que ha sido procesado. Por otra parte los auditores del sistema pueden verificar que todos los votos emitidos han sido publica-

dos y correctamente descifrados, gracias al mecanismo criptográfico que recupera la posición de los candidatos.

Desde el punto de vista del votante el proceso de votación tiene varios pasos:

- Emitir el voto. Para ello debe recoger una boleta, marcar su elección en la columna de la derecha, cortar la parte izquierda y destruirla de alguna forma fehaciente para que no sirva de instrumento que demuestre lo que se ha votado y escanear la parte derecha en la urna electrónica.
- Comprobar, con ayuda de la mesa y de forma opcional una boleta con el fin de comprobar que el número de serie de la misma permite recuperar el orden de los candidatos.
- Verificar el voto, reteniendo la parte derecha del mismo (o una copia) una vez escaneado a modo de recibo con el objeto de comprobar que coincide con el que aparece en el tablón de anuncios una vez cerrada la votación. Así mismo puede ser utilizado como prueba en caso de impugnación de la votación si no apareciera o se mostrara modificado.

La idea básica de este sistema es que los votos emitidos están cifrados de la misma forma que aquellos que son descifrados previamente para comprobar su correcto funcionamiento y la imposibilidad de realizar la trazabilidad sobre los mismos, incluidas las autoridades electorales. Para ello se utilizan tres pasos que pueden realizarse separados o combinados y son: el mezclado o barajado de los votos, el descifrado y el recuento. Para verificar el proceso se eligen al azar y públicamente una

serie de votos, que son utilizados para demostrar que el proceso es fiable y preciso. El proceso de comprobación previo para confirmar el correcto funcionamiento del sistema, en ningún caso pone al descubierto los detalles del procedimiento pero permite al votante comprobar que su voto ha sido grabado como él ha elegido y posteriormente ha sido contabilizado como fue depositado, aspecto este que en principio sólo está garantizado por el correcto diseño del algoritmo de cifrado/descifrado.

Para ello utiliza una forma particular de permutación por desplazamiento cíclico de la lista de candidatos que se repite en varias ocasiones formando varios procesos continuados de cifrado en forma de "capas de cebolla" impidiendo el proceso inverso salvo que se conozca el algoritmo completo, al cual nadie tiene acceso directamente, salvo el sistema en el momento del recuento cuando es activado mancomunadamente por los miembros de la mesa.

Al igual que en el caso del PunchScan la codificación entre las capas se hace cifrando las referencias con RSA, constituyendo las denominadas *tellers* que son unas tablas cifradas encargadas de enlazar la información entre las diversas capas, es decir son *mixnets*. Estas *tellers* permiten la progresión del cifrado en un sentido pero la impiden en sentido contrario salvo que se conozcan las claves. De esta forma se impide relacionar las marcas leídas por el OCR con la posición de los candidatos u opciones de la boleta en concreto. El número de serie de la boleta es el encargado de iniciar el cifrado de la posición

de los candidatos, de tal forma que aun conociendo este número y la posición de las marcas es inviable recuperar la lista original, aun en el caso de conocer los detalles del encriptado. Para poder recorrer las capas en sentido contrario con el objeto de realizar el recuento es necesario conocer las diversas claves entre cada capa.

Es importante separar las boletas utilizadas para comprobar el correcto funcionamiento del proceso, de las que se van a utilizar para votar. En particular supondría un problema contra el secreto del voto utilizar una copia de una boleta que haya sido usada para votar y posteriormente proceder con la copia a su verificación, descubriendo de esta forma el sentido del voto. Esto se puede evitar comprobando en el momento del escaneo que el número de serie no haya sido utilizado previamente.

El sistema permite en su última versión una boleta de opción múltiple e incluso con orden de preferencia, haciendo figurar un número en vez de una simple marca.

C.6.- Bingo Voting

El Bingo Voting es un sistema de votación electrónica que fue introducido en 2007 por Jens- Matthias Bohli, Jörn Müller- Quade y Stefan Röhrich pertenecientes al Instituto de Seguridad y Cifrado (IKS) adscrito al Instituto de Tecnología de Karlsruhe (KIT) en Alemania. (BOHLI, 2007). En 2008 fue galardonado con el premio alemán sobre seguridad de la Fundación Horst Görtz. Posteriormente se introdujeron mejoras basadas en la tesis doctoral de Christian Henrich. En ésta se presenta

la versión original del Bingo, se describe la experiencia adquirida durante la primera elección en el mundo real llevado a cabo en las elecciones de los representantes de los estudiantes de la Universidad de Karlsruhe en el 2008 y propone varias mejoras para abordar algunas deficiencias y debilidades.

La votación se desarrolla sobre una urna electrónica tipo DRE que después de la elección del votante emite un recibo. Por tanto no hay boletas de papel. La urna utiliza un generador de números aleatorios para cifrar los votos y para su emisión se usan dispositivos de confianza, así denominados por los autores, como podrían ser una pantalla táctil y una impresora laser. Igualmente esencial son sus recibos en papel sin información sobre el sentido del voto, lo que viene a denominarse "recibo anti-coacción" (freeness receipt), para evitar la compra de votos y la intimidación pero que permiten al votante verificar que su voto fue procesado correctamente. En este recibo sólo figuran los nombres de los candidatos con un número a continuación. Por tanto todo el proceso de votación, se desarrolla sobre una urna electrónica con una interfaz gráfica genérica y una impresora de recibos.

La idea central de Bingo Voting es que la urna cifre la elección del votante mediante la generación de números aleatorios para cada una de las opciones. Hay dos tipos de números aleatorios en el proceso, los números aleatorios "ficticios" (dummy) generados antes de la fase de votación y números aleatorios "recientes" (fresh) que se generan durante el proceso de votación mediante el generador

de números aleatorios de confianza. El número aleatorio utilizado para codificar la elección final del votante se genera como número aleatorio “reciente” y es mostrado por el generador de números aleatorios de confianza dentro de la cabina de votación. El resto de los números en el recibo del votante son números aleatorios “ficticios”.

Los números aleatorios ficticios son los números que aparecen en el recibo y que además no se corresponden con ninguna elección del votante. Es importante recalcar que estos números se fijan antes de que comience la fase de votación. Si suponemos una elección en la que participen N votantes (donde cada votante puede emitir un único voto), cada candidato tendrá inicialmente N números aleatorios ficticios distintos.

Los números aleatorios recientes (generados durante la fase de votación por el generador de números aleatorios de confianza) son los que se utilizan para identificar en el recibo la elección realizada por el votante en la urna electrónica en el momento de la votación. El algoritmo utilizado para la generación de estos números recientes, que son los que finalmente aparecerán en el recibo del votante señalando la opción escogida, no garantiza que anteriormente no hayan sido utilizados en el grupo de los ficticios, es decir, que no hayan sido generados antes. Si esto ocurriera se denominan “colisiones” (una en el caso de 100.000.000 votantes, con una longitud de los números aleatorios de 30 bits y con una probabilidad de ser detectada del 0,99995).

En la descripción del proceso de votación es fácil imaginar que todo depende del engaño que establecemos al considerar que los votos ficticios puedan representar votos reales. En la fase de preparación de la votación se adjudican el mismo número de votos ficticios a cada candidato. Durante la fase de votación y cada vez que un votante elige al candidato Z, ese candidato NO pierde un voto ficticio ya que es reemplazado por un número aleatorio reciente. Esto significa que el candidato Z tiene ahora un voto ficticio MÁS que los otros candidatos. Por esta razón, el número de votos ficticios que le quedan a cada candidato se traduce directamente en el resultado del recuento, si al comienzo de la votación cada candidato tenía tantos votos ficticios como votantes.

Para que todo funcione como se espera tenemos que garantizar dos cosas. Lo primero es que podamos demostrar que todos los candidatos dispongan inicialmente del mismo número de votos ficticios y la autoridad electoral lo pueda comprobar. Este valor debería ser como mínimo igual al número máximo de votantes, pero podría ser superior sin problema. El segundo aspecto que es necesario cuidar es que cada vez que se vota por un candidato hay que restar un voto ficticio.

En cambio para demostrar que por cada voto emitido no se le descuenta uno ficticio al candidato elegido, deben darse dos pasos. Primero, para generar el recibo, la urna imprime un número aleatorio ficticio al lado de cada candidato no votado y un número aleatorio reciente al lado del nombre del candidato votado y que es calculado por el generador de números aleatorios recientes en

ese instante. El votante es capaz de comprobar esto, comparando la pantalla del generador de números recientes con lo impreso en el recibo, de forma que ese número debe aparecer al lado del nombre de su candidato. En un segundo paso, el votante puede verificar por medio de la publicación que hace la autoridad electoral al final del proceso y mediante el listado de todos los números ficticios que no han sido "consumidos" y por tanto utilizados para el recuento, que cada número que figura al lado de cada candidato en su recibo no está incluido en la lista y por tanto cada uno de ellos ha "consumido" un voto ficticio o bien ha utilizado un número "reciente".

Antes de la fase de votación la autoridad electoral publica los requisitos de la votación. Esto incluye la lista de candidatos y el número de votos ficticios asociados a cada uno de ellos. Se supone que la máquina que genera los números ficticios utiliza el mismo sistema que para los números aleatorios recientes, aunque estos últimos utilizan un algoritmo que intenta impedir la repetición de los ya generados.

Suponiendo una elección en la que participen N votantes y donde cada votante puede emitir un voto, dicha máquina generará N números aleatorios ficticios en función del número de votantes para cada candidato y guardará este conjunto de números ya que es necesario para realizar el recuento y generar los recibos. Es importante recalcar que además del conjunto de votos aleatorios ficticios, la máquina de votación lleva a cabo una prueba para mostrar que cada candidato ha recibido el mismo número de votos ficticios. Además el número de votos

ficticios debe coincidir exactamente en todos los candidatos y debemos garantizar que en ningún caso este listado pueda hacerse público. Sólo entonces puede comenzar la fase de votación.

El votante una vez verificada su identidad entrará en la cabina de votación y activará el sistema mediante una *smart card* y se encontrará con una mesa con una pequeña impresora para emitir el recibo, la máquina de votación tipo DRE con pantalla y ratón y el generador de números aleatorios recientes conectado a la máquina de votación. Después emite su voto con ayuda del ratón e inmediatamente después el generador de números aleatorios recientes proporciona un número para el candidato elegido. El elector lo verifica y presiona la opción de VOTAR y se imprime un recibo asignando el número aleatorio reciente al candidato elegido. En este punto es importante señalar que Alice no pierde un voto ficticio por lo que tiene un voto ficticio más comparado con el resto de candidatos que sí los "consumen" y de esta forma podemos realizar posteriormente el recuento.

¿Cómo verifica el usuario que su voto ha sido emitido correctamente? Comparando el número visualizado en la pantalla del generador de números aleatorios de confianza con el número asociado al candidato que él ha elegido. Sólo el votante sabrá quién ha sido el candidato elegido ya que para cualquier otra persona ese número es indistinguible de los números aleatorios ficticios.

Durante la fase de recuento la autoridad electoral publica tres conjuntos de datos distintos:

- Una copia digital de cada recibo emitido durante la fase de votación. De esta forma cada votante puede verificar que su voto fue emitido y publicado correctamente.
- Se demuestra para cada recibo publicado que contiene la cantidad correcta de números aleatorios de cada tipo, es decir, que todos menos uno (el número aleatorio reciente) son números aleatorios ficticios. Esta comprobación la hace la mesa electoral mediante un proceso cerrado y supuestamente fiable.
- La autoridad electoral publica todos los números aleatorios ficticios que no fueron utilizados durante el proceso de votación. Estos votos se denominan votos ficticios restantes y son los que se utilizan para hacer el recuento.

Lo verdaderamente importante es que el número de los votos ficticios restantes para cada candidato tiene correspondencia inversa con el número de votos que este candidato recibió durante la fase de votación, a partir del cual obtenemos directamente el recuento de ese candidato.

¿Cómo se obtiene el recuento? En primer lugar, restando al número de votos ficticios de cada candidato, el número de personas que no votaron, es decir, el número de votantes para los que la autoridad electoral creó números aleatorios ficticios pero que no fueron utilizados. Estos datos pueden ser calculados a partir del número de recibos publicados que equivale obviamente al número

de votos emitidos. En segundo lugar, el número de números aleatorios ficticios que le quedan a cada candidato será el número de votos recibidos por cada uno de ellos.

¿Cómo tener en cuenta los votos en blanco y votos inválidos?

- Lógicamente si no se ha elegido candidato en el voto, en el recibo no debería existir ningún número aleatorio reciente, por lo que el comprobante sólo tendrá números ficticios asociados a los candidatos que habrían sido utilizados por todos ellos. Inmediatamente marcaríamos la boleta como un voto en blanco que habría que tener en cuenta como un voto que no se contabiliza para ningún candidato. Otra opción sería crear un "candidato en blanco".
- Como no es posible que el recibo contenga más de un número aleatorio reciente, esta opción no existe.

Existen dos tipos de verificaciones, la individual y la global.

La verificación individual tiene dos partes:

- En la primera de ellas, durante la fase de votación, el votante comprueba que en su recibo se codifica correctamente el candidato seleccionado, comparando el número aleatorio generado en ese momento por el generador de confianza y que es asignado al candidato elegido en el recibo que recoge el votante.
- En la segunda, después de la fase de votación, el votante verifica que su recibo se ha publicado correc-

tamente. Si el recibo emitido durante el proceso de votación es idéntico al recibo publicado posteriormente por la autoridad electoral, puede deducirse que el voto fue incluido en el recuento, aunque no tenemos garantías de que haya sido contabilizado correctamente.

Para cumplir con la verificación global la autoridad electoral tiene que comprobar:

- Que cada candidato cuenta al principio de la votación con idéntico número de votos ficticios y esto se lleva a cabo mediante una comprobación aleatoria parcial.
- Que cada recibo está correctamente creado y que todos los números son ficticios salvo uno, o dicho de otra forma, que cada candidato no votado perdió como máximo un número ficticio por cada votante. Esto se realiza verificando que todos los números aleatorios del recibo menos uno son ficticios mediante un procedimiento que los miembros de la mesa pueden ejecutar.
- Que cada número ficticio generado inicialmente figura en un recibo (ha sido consumido) o bien está publicado como no utilizado en el proceso (ficticios restantes).
- Por último ha de comprobarse que el número de coincidencias (colisiones al generar los números aleatorios) es mínimo y que en ningún caso puede afectar al resultado.

El núcleo de esta votación se fundamenta en el carácter imprevisible del generador de números aleatorios de

confianza (TRNG) y en los estrictos compromisos de privacidad entre el voto y el votante. Para ello es esencial que todos los números aleatorios ficticios sean únicos y esta es la razón de la comprobación de todos los números ficticios generados en la fase de preparación. De esta forma es bastante sencillo detectar las posibles repeticiones al generarse aleatoriamente los números recientes. Si no podemos asegurar la unicidad, es importante al menos asegurar que habrá muy pocas repeticiones, ya que cada colisión significa un voto potencialmente modificado. Esto debe ser comprobado en cada mesa mediante un procedimiento que se ejecutará antes de la votación. El número de colisiones que se considera aceptable se determina por el número de votos que pueden cambiarse sin alterar el resultado de la elección, pero pueden existir.

Como la mayoría de los sistemas de votación con verificación de extremo a extremo, este exige la publicación de los datos que permitan verificar la exactitud de los resultados y convencer a los votantes de que su voto se incluyó correctamente en el recuento. Para ello se publican los números ficticios restantes mediante un servicio web y una copia de cada uno de los recibos.

El recibo anti-coacción se basa en la imposibilidad de distinguir entre números aleatorios ficticios consumidos y los recientes, así como en el cuidado aislamiento de la cabina de votación y de la urna que se utiliza para votar.

Es evidente que en este sistema es crítico el diseño del generador de números aleatorios y por ello originalmente se propuso un sistema mecánico como los utilizados en el juego del bingo. Ahora la propuesta es generarlos

a partir de una tarjeta criptográfica. Para que el método funcione correctamente, los números aleatorios ficticios deben ser calculados de forma que puedan verificarse antes de que comience la fase de votación. En cuanto al recibo anti-coacción, debe mantenerse en secreto qué número aleatorio es el reciente y cuáles se han generado antes de la votación. Para garantizar estas propiedades el sistema utiliza un esquema de compromisos mediante un algoritmo denominado UHDLC.

También es importante para el correcto funcionamiento que todos los números aleatorios sean únicos y ésta puede ser una debilidad ya que el sistema no lo garantiza. Dado que cada repetición puede significar que un voto ha sido modificado, el número de repeticiones queda fijado por el número de votos que pueden cambiarse sin alterar el resultado de la votación. Esta información se publica al final del recuento.

BIBLIOGRAFÍA

· ADDER,J (2014) "http://cryptodrm.engr.uconn.edu/adder/index.shtml". (Último acceso: 03/03/ 2015).

· ADIDA B. y RIVEST R. L. (2006), "Scratch & Vote: Self-Contained Paper-Based Cryptographic Voting", ACM Workshop on Privacy in the Electonic Society, ACM.

· ADIDA B., (2006) "Advances in cryptographic voting systems". Thesis Ph. D.Massachusetts Institute of Technology, Dept. of Electrical Engineering and Computer Science.

· Araya, Rodrigo y Miguel Porrúa. (2004). "América Latina Puntogob. Casos y tendencias en gobierno electrónico". Flacso.Santiago.

· AYCART PÉREZ , D GINESTÀ, M MATÍAS, M Y HERNÁNDEZ, J (2007) "Ingeniería del software en entornos de Software Libre". Eureca Media. Barcelona

· BARGACH, CLAUDIO (compilador) y ot. autores, (2015), "Ser fiscal. Una reforma electoral como política de Estado". Red de Encuentro Ciudadano para la calidad Democrática,

· BAUDRON O. y et al.(2001), "Practical multi-candidate election system,» PODC de ACM.

· BENALOH J. (2006), "Simple verifiable elections", EVT'06 Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop.

· BISMARK,D., J. HEATHER, R. M. A. PEEL, S. SCHNEIDER Y P. Y. RYAN, (2009), "Experiences Gained from the first Prêt à Voter Implementation", Requirements Engineering for e-Voting Systems (RE-VOTE), vol. 1, nº 1.

· BOHLI J. M., J. MÜLLER-QUADE Y S. RÖHRICH, (2007),"Bingo Voting: Secure and Coercion-Free Voting Using a Trusted Random Number Generator", VOTE-ID 2007, LNCS 4896.

· Boltz y Centeno Laopas, (2012), “El ejemplo de Australia en los comicios de 2001¨Revista Mexicana de Análisis Político y Administración Pública, Universidad de Guanajuato, Vol.1, n° 2.

· Boltz, I. y Centeno Lappas, F. (2005). “Riesgos y debilidades del voto electrónico: en busca de transparencia, seguridad y confianza en el proceso electoral”, en María Inés Tula (Ed.), “Voto Electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales”, Ed. Ariel, Buenos Aires.

· CALIFORNIA INSTITUTE OF TECHNOLOGY, (2006) “http://electionupdates. caltech.edu /2006/12/18/threeballot-tested-by-mit-students/”. [Ref consulta con acceso: 29 01 2014]. en «http://caltech.edu/,»

· CARBACK R. T. III, (2010), “Engineering Practical End-to-End Verifiable Voting Systems”. Thesis MD, Baltimore: University of Maryland, Baltimore County (UMBC), 2010.

· CARBACK R., D. CHAUM, J. CLARK Y et al.(2010), “Scantegrity II municipal election at Takoma Park: the first E2E binding governmental election with ballot privacy”, USENIX Security’10 Proceedings of the 19th USENIX conference on Security.

· CHAUM D. Y CARBACK R. ,(2006), “http://www.punchscan.org/”, (En línea: http://www.punchscan.org/) . [Último acceso: 29 04 2016].

· CHAUM D.,(2004), “Secret-ballot receipts: True voter-verifiable elections”, Security and Privacy.

· CHAUM D.,(1981), “Untraceable electronic mail, return addresses, and digital pseudonyms”, Magazine Communications of the ACM, vol. 24, nº 2.

· CHAUM D., P. Y. A. RYAN Y S. SCHNEIDER, (2005), “A practical voter-verifiable election scheme”, Proceedings of the 10th European conference on Research in Computer Security, vol. 1, nº 1.

· CHAUM D., R. CARBACK, S. POPOVENIUC, R. L. RIVEST Y P.

Y. RYAN, (2008), “Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes”,» [En línea; https://www.usenix.org/legacy/event/evt08/ tech/full_papers/chaum/chaum.pdf. [Último acceso:01 05 2016].

· Clemente, A. (2007) “Las Boletas Electorales¨ en Tratado de Derecho Electoral Comparado de América Latina” Comp. Nohlen, Zovatto, Orozco, Thompson; Capítulo XXXV, FCE, México.

· Corte Constitucional Alemana (2009) “Fallo BvC 3/07 – 2BvC 4/07-, pronunciado el 3 de marzo de 2009 en el proceso de Queja de Control Electoral contra la resolución del Bundestag Alemán del 14 de diciembre de 2006”, Justicia Electoral, Revista del Tribunal Electoral del Poder Judicial de la Federación, Cuarta Epoca, Vol. 1, núm. 6, 2010, México, . Traducción de Manfredo Koessl).

· ESSEX A., J. CLARK, R. T. I. CARBACK Y S. POPOVENIUC,(2010) “http://punchscan.org” [En línea]. Available: http://punchscan.org/vocomp/PunchscanVocompSubmission.pdf. [Último acceso: 26 01 2016].

· FINK R. A. Y SHERMAN A.(2009), “Combining end-to-end voting with trustworthy computing for greater privacy, trust, accessibility, and usability”, Proceedings of the National Institutes of Technology (NIST) workshop on end-to-end voting systems.

· FINK R. A.(2010), “Applying Trustworthy Computing to End-To-End Electronic Voting”. Thesis, University of Maryland, Baltimore County.

· FISHER K., R. Carback y A. Sherman, «Punchscan: Introduction and System Definition of a High-Integrity Election System,» Proceedings of the IAVoSS Workshop On Trustworthy Elections (WOTE 2006), 2006.

· GOBIERNO VASCO, (2015) “Voto Electrónico en el mundo¨ Dirección de Régimen Jurídico, Servicios y Procesos Electorales. [En línea: http://www.euskadi.eus/botoelek/ve_mundo_c.htm] . [Último acceso: 05 04 2016]

· Gómez, Ana y Justo Carracedo. (2006). “Del voto electrónico al voto telemático: clasificación y valoración de las propuestas existentes.” Universidad Politécnica de Madrid

· Gómez, Ana y otros. (2006). “Planteamientos sobre voto electrónico y Democracia Electrónica”. Universidad Politécnica de Madrid y Universidad Complutense de Madrid.

· KIAYIAS A., M. Korman y D. Walluck, (2006), “An Internet Voting System Supporting User Privacy”, Computer Security Applications Conference, vol. 22, nº 1.

· Lévy, Pierre. (2004). “Ciberdemocracia”. Ensayo sobre filosofía política.

· PAILLIER P., (1999), “Public-key cryptosystems based on composite degree residuosity classes”, Lecture Notes in Computer Science.Volume 1592, Springer.

· PANIZO ALONSO, L (2013) “Libro blanco sobre el voto electrónico”. Plataforma votoe.es. disponible en http://hdl.handle.net [Último acceso: 26 01 2016].

· PANIZO ALONSO, L (2014) “Desarrollo de una metodología para el análisis y la clasificación de los sistemas de voto electrónico” Tesis doctoral Universidad de León Departamento de Ingeniería Eléctrica y de Sistemas y Automática

· Pérez Corti, J. (2010). “Los principios generales del derecho electoral y su gravitación en la inconstitucionalidad del régimen alemán de voto electrónico”, en http://www. te.gob.mx/documentacion/publicaciones/Justicia_electoral/juel_a6_n2_1.pdf [Ultimo acceso 15 04 2016]

· POPOVENIUC S. Y HOSP B.,(2010), “An Introduction to PunchScan, Towards a Trustworthy Elections”. Lecture Notes in Computer Science Volume 6000, Berlin, Springer Berlin Heidelberg.

· POPOVENIUC S. Y HOSP B., (2010) “PunchScan”» (En línea: http://popoveniuc.com/papers /PunchScan.pdf. [Último acceso: 25 04 2016].

· POPOVENIUC S., J. M. KELSEY, A. R. REGENSCHEID Y P. VORA, (2010), “Performance Requirements for End-to-End Verifiable Elections”, Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE ‘10), Washington.

· PRÊT Á VOTER, (2005) “pretavoter” . [En línea: http://www.pretavoter.com/. [Último acceso: 26 03 2016].

· Prince, A. Jolías, L. y Lacabanne, F (2012)- “Voto electrónico en Argentina”, 6to. Simposio Argentino de Informática en el Estado. 41 JAIO. ISSN. 1851-2526.

· Rial, Juan. (2006). “Modernización del proceso electoral: el voto electrónico. Observatorio electoral”. Disponible en :www.observatorioelectoral.org/biblioteca/?bookID=26&page=11>.[Último acceso: 26 03 2016].

· RIVEST R. L. y Smith W. D.,(2007) “Three voting protocols: ThreeBallot, VAV,and Twin “, EVT’07 Electronic Voting Technology Workshop, Boston.

· RIVEST R. L., (2006), “The ThreeBallot Voting System”, (En línea: http://theory.csail.mit.edu/ ~rivest/Rivest-TheThreeBallotVotingSystem.pdf. [Último acceso: 26 03 2016].

· Romero Flores y Tellez Valdez, (2012). “Voto Electrónico”, Revista Mexicana de Análisis Político y Administración Pública, Universidad de Guanajuato, Volumen 1, número 2.

· RYAN P. Y. A., D. BISMARK, J. HEATHER Y S. SCHNEIDER, (2009), “Prêt à Voter: a Voter-Verifiable Voting System”, Information Forensics and Security, vol. 4, nº 4.

· RYAN P. Y., (2007), “Pret a voter with a human-readable, paper audit trail”, Frontiers of Electronic Voting, Schloss Dagstuhl, Germany.

· RYAN P. Y., D. BISMARK, J. HEATHER Y S. SCHNEIDER, (2009), “Prêt à Voter: a Voter-Verifiable Voting System”, Information Forensics and Security, vol. 4, nº 4.

· SHERMAN A. T., R. A. FINK, R. CARBACK Y D. CHAUM, (2011), “Scantegrity III: automatic trustworthy receipts, highlighting over/under votes, and full voter verifiability”, EVT/WOTE’11 Proceedings of the 2011 conference on Electronic voting technology/workshop on trustworthy elections.

· Stallman, R. ,(2004), “Software libre para una sociedad libre”, Ed. Traficantes de Sueños ISBN: 84-933555-1-8

· TRUSTWORTHY VOTING SYSTEMS (2016), «http://www.tvsproject.org/,» [En línea: http://www.tvsproject.org/ . [Último acceso: 05 04 2016].

· Tula, M. (2005) “Voto electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales”. Buenos Aires, Ed. Ariel.

· Tula, M. (2007) “Apuntes y recomendaciones para el estudio del voto electrónico en la provincia de Córdoba”. WP.

· UNITED STATES ELECTION ASSISTANCE COMMISSION, (2014) ,”Voting system perfomance guidelines”, [En línea: http://www.eac.gov/assets/1/workflow_staging/Page/124.PDF. [Último acceso: 21 03 2016].

· WINCKLER M., R. BERNHAUPT, P. PALANQUE et al.(2009), “Assessing the Usability of Open Verifiable e-Voting Systems”, Proceedings of the 1st International Conference on eGovernment and eGovernnace (ICEGOV)., Ankara, Turquía.

LOS AUTORES

MOLINA, ALEJANDRO HECTOR

Ingeniero Electricista, Magister en Políticas y Estrategias y Doctor en Ingeniería por la UNS. Docente Investigador UTN FRBB. Docente de Grado y Post Grado UNS y UTN FRBB. Consultor en Ingeniería y Sistemas. Especialista en Medio Ambiente CIPBA. Ex Analista de Sistemas de Cómputos en la Armada Argentina. Ex Perito de la CSJPBA. Miembro de la RED SER FISCAL. Coordinador del Grupo de Tecnologías Electorales de la RED SER FISCAL.

BOTTONI, MABEL NOEMI

Química e Ingeniera Química por la UNS. Auditora y Especialista en gestión de la calidad Ambiental IRAM. Especialista en Medio Ambiente CIPBA. Consultor en Ingeniería y Sistemas. Docente UNS, UTN FRBB, Academia de Policía de Bahía Blanca e ISFT Nº 190. Miembro de la RED SER FISCAL. Miembro del Grupo de Tecnologías Electorales de la RED SER FISCAL.

GARCIA, CLAUDIA LILIAN

Abogada por la UBA. Mediadora. Diplomada en Tecnologías y Derecho aplicados a Procesos Ambientales del ITBA. Docente invitada en la UCES y en la UBA (de Grado y Post Grado). Vicepresidente de la Asociación Civil Democracia y Consenso (DEYCON). Coordinadora Nacional Legal de la RED SER FISCAL

EL EQUIPO DE SER FISCAL

BARGACH, CLAUDIO C.

Psicólogo Social. Director Profesional de la YMCA. Presidente de la Red Encuentro Ciudadano para la calidad Democrática (REC) Coordinador Nacional de la Red SER FISCAL.

COLABORADORES

BUFFONE, FERNANDO

Licenciado en Organización Industrial. Secretario de Asuntos Estudiantiles UTN FRBB. Docente investigador UTN. Miembro del Grupo de Tecnologías Electorales de la RED SER FISCAL.

MOLINARI, VICTORIANO

Licenciado en Organización Industrial. Docente investigador UTN. Miembro del Grupo de Tecnologías Electorales de la RED SER FISCAL.

EVALUADOR

GUTIERREZ , RICARDO

Profesor titular Dpto Economía UNS. Docente investigador Cat. I MinCyT. Se ha desempeñado como consultor económico y en el ámbito académico. Profesor de Postgrado en materias como “Política Tecnológica”, “Teoría Política”, “Instituciones jurídicas y organización del Es-

tado", "Instituciones jurídicas y organización del Estado" y otras pertenecientes al área de economía. Ha actuado en funciones de gestión y dirección de la UNS, como Director Decano del Dpto. De Economía, Miembro de Consejo Superior y Rector entre los años 1994 y 2000. Participó en el sistema de educación superior en funciones como Miembro Consejo Permanente Interuniversitario de Ciencia y Técnica, Miembro de la Comisión Asesora PATCYT. Representante de UNS ante Comisión Interuniversitaria para la Integración Latinoamericana. Autor de diversos trabajos de investigación, libros y publicaciones. Director de varias tesis de grado y postgrado.