CONSIDERACIONES SOBRE EL VOTO ELECTRÓNICO

MIGUEL MONTES[1], DANIEL PENAZZI[2], Y NICOLÁS WOLOVICK[3]

RESUMEN. El voto electrónico es un tema que se ha instalado tanto en las agendas de gobierno (nacional, provincial y municipal) como en la opinión pública. Este trabajo discutimos algunas posibles definiciones de voto electrónico; analizamos algunas debilidades, tanto prácticas, según revelan algunas experiencias en el mundo, como teóricas; y postulamos una serie de requerimientos que a nuestro criterio debería cumplir cualquier sistema de este tipo.

1. INTRODUCCIÓN

El voto es el mecanismo mediante el cual los ciudadanos de una democracia representativa, como la de la República Argentina, eligen a sus representantes. Es una condición necesaria para el funcionamiento de un sistema democrático y el más básico de los derechos políticos, por lo que es esencial que cualquier sistema de votación que se utilice preserve las características establecidas en nuestra Constitución: "El sufragio es universal, igual, secreto y obligatorio" [1].

En los últimos tiempos han surgido numerosas críticas a los sistemas convencionales de votación. Muchos de los problemas citados son de larga data. No es el objetivo de este trabajo analizarlos, pero merecen mencionarse el "voto en cadena", el robo de boletas o el uso de boletas numeradas en sistemas de boleta única [2, 3].

Una de las críticas más frecuentes en los últimos procesos electorales se centran en la lentitud del conteo provisorio, y se plantea como solución obvia el uso del voto electrónico. Si tantos trámites en nuestra vida se han visto acelerados por el uso de computadoras, ¿por qué no acelerar de la misma manera el escrutinio?. Si existen cajeros automáticos, ¿por qué no urnas automáticas?.

Si bien la rapidez del escrutinio es claramente una característica deseable, está lejos de ser esencial, y no puede imponerse sobre los requisitos ineludibles de universalidad, igualdad y confidencialidad.

Sin embargo, el tema está instalado, y forma parte de la agenda del Gobierno Nacional y de muchos gobiernos provinciales. El presente trabajo pretende ser un aporte en este sentido. En primer término definimos los distintos tipos de sistemas de voto electrónico existentes, luego analizamos algunos de sus problemas, y finalmente proponemos una serie de requerimientos que consideramos deben ser satisfechos por cualquier sistema de voto electrónico que se implemente.

1:UNIVERSIDAD NACIONAL DE CÓRDOBA, INSTITUTO UNIVERSITARIO AERONÁUTICO

2:CIEM-FAMAF, UNIVERSIDAD NACIONAL DE CÓRDOBA

3:FAMAF, UNIVERSIDAD NACIONAL DE CÓRDOBA

E-mail addresses: mmontes@iua.edu.ar, penazzi@famaf.unc.edu.ar, nicolasw@famaf.unc.edu.ar.

2. Definiciones y terminología

2.1. Etapas del proceso de votación. En el proceso de votación de un sistema de voto moderno pueden distinguirse tres etapas:

Creación del voto: el elector selecciona de alguna forma entre las opciones disponibles y "crea" el voto, en algún formato.

Resguardo anónimo del voto: el voto es resguardado junto con otros votos para anonimizarlo.

Conteo de los votos: luego de concluido el tiempo disponible para votar, se cuentan los votos resguardados.

La informatización de una o más etapas nos permite llegar a una definición:

Definición 1. Una definición posible es llamar *Voto Electrónico* a cualquier sistema que introduzca computadoras en alguna de esas etapas. Otra definición más minimal es llamar *Voto Electrónico* a sistemas en donde la emisión del voto es electrónica y *Conteo electrónico* si las computadoras sólo se usan en el conteo.

2.2. DREs e IREs. En algunos sistemas de Voto Electrónico tanto la emisión como el conteo de votos se hacen en una sola máquina. Estos sistemas suelen llamarse DRE (*Direct-Recording Electronic voting machines*), o también Urnas Electrónicas. En algunos casos estos sistemas proporcionan registros de auditoría en papel (*paper audit trail*).

Otros sistemas usan la idea propuesta por Bruck, Jefferson y Rivest [4] y separan físicamente la generación del voto de su conteo: el elector crea de un objeto físico que representa su voto (un *token* o boleta), y éste es depositado en una urna para ser contado posteriormente, ya sea de forma manual o electrónica. Suelen ser llamados *Electronic Ballot Printers* (EBP) [5, 6] o *Indirect-Recording Electronic voting machines* (IRE) [7].

La característica técnica que distingue los DREs de los EBPs no es la emisión o no de una boleta impresa. Como se mencionó antes, algunos DREs imprimen una boleta de papel, ya sea guardando esa boleta directamente en la misma máquina o entregándosela al votante para que la deposite en una urna común. La diferencia fundamental es que en los DREs la misma máquina que genera el voto lo cuenta por lo cual no existe el proceso de separación entre la emisión individual del voto y el conteo anónimo dado por el paso intermedio de guardar las boletas en la urna. Los DREs son peligrosamente cercanos al voto cantado, solo que el que cuenta los votos individualizados es una máquina en vez de un ser humano. Para evitar este peligro, los DREs deben tener sistemas adicionales que no permitan reconstruir los votos individuales a partir de los registros internos de la máquina, pero el votante no puede verificar por sí mismo que esos sistemas sean seguros.

En cambio, los IREs mantienen la separación tradicional entre la emisión individual del voto y el conteo anónimo del mismo, provisto por la mezcla de cada voto con otros votos en la urna. Los IREs

no necesitan guardar ningún dato sobre el voto que generan mientras que los DREs necesariamente deben hacerlo. Esto hace que los IREs sean más seguros que los DRE, aunque los costos pueden ser mayores.

En Argentina algunas personas llaman Voto Electrónico sólo a los DREs y a los EBPs los llaman Boleta Electrónica.

En una ley que incluya la aplicación del voto electrónico debería quedar claro cual definición de voto electrónico se usa. Además, hay que tener cuidado en que la ley no favorezca el producto de una empresa específica. Por ejemplo, sería recomendable que no se requiera un sistema de Boleta Única Electrónica, ya que ese término ha quedado vinculado al sistema Vot.ar propuesto por la empresa MSA.

3. Problemas con el Voto Electrónico

El Voto Electrónico tiene problemas tanto a nivel práctico como a nivel teórico.

3.1. Problemas a nivel práctico. Cualquier programa complejo tendrá inevitablemente errores, incluyendo programas hechos por empresas como Apple, Microsoft o Bethesda.

En el caso del voto electrónico, además de los errores, tenemos que lidiar con posibles ataques internos que traten de esconder un fragmento de código malicioso. Como ejemplos de errores o malicia podemos mencionar:

- Se cuentan mal los votos.
- Se registran mal los votos (el elector elige A pero el sistema registra B, o nada).
- Se revela el voto de uno o más electores.
- Se cuentan múltiples votos para un mismo elector.
- Se registran votos no emitidos por ninguna persona (análogo a la “urna embarazada”).
- Máquinas o software que han sido examinados son reemplazados en la elección por otros que no han sido auditados.
- Se usan técnicas inadecuadas de seguridad.

Uno de los ejemplos más destacados es lo ocurrido en Volusia County, Florida, en las elecciones presidenciales de los Estados Unidos del año 2000: Gore recibió -16.022 votos (votos negativos) [8]. Aunque este error luego fue subsanado, provocó que las cadenas nacionales anunciaran antes de tiempo que Bush era el ganador.

En 2003, en Boone County, Iowa, un condado de 50.000 habitantes de los cuales menos de la mitad estaban habilitados para votar, el equipo electrónico contó 140.000 votos [9].

Más recientemente en 2015 se descubrieron múltiples problemas en el sistema AVS WinVote [10], entre ellos que tiene contraseñas débiles que no pueden ser cambiadas, utiliza Wired Equivalent Privacy (WEP) (mostrado inseguro en 2001 y reemplazado por WPA desde 2003), y usa una versión de Windows XP Embedded que no ha sido actualizada desde 2004.

El sistema usado en Brasil fue analizado por Diego Aranha [11], quien encontró que se puede saber quien votó a quien por una mala implementación del mecanismo de aleatoriedad que supuestamente oculta el orden en el cual los votos fueron emitidos por los votantes. Además Aranha mostró que el sistema de verificación de identidad del votante está enlazado con la máquina de votación, que los algoritmos criptográficos son obsoletos, que el sistema es vulnerable a amenazas internas, que hay fallas en el uso de mecanismos de cifrado, etc.

Al sistema Vot.ar, utilizado en la Ciudad Autónoma de Buenos Aires, se le encontraron también varias fallas [12, 13]. Entre otros problemas, los investigadores encontraron que las boletas pueden ser individualizadas, se puede generar una boleta que contenga más de un voto, y el voto puede ser leído por un celular llevado por el votante con solo acercar el celular a la boleta, permitiendo la compra de voto. Si bien los chips RFID que utiliza el sistema están diseñados para ser leídos sólo a poca distancia (centímetros), se ha demostrado la posibilidad de aumentar la distancia de lectura a decenas de metros (*extended range attack*), lo cual permitiría leer los votos aún sin la colaboración del votante, o realizar otros ataques, como por ejemplo anular o cambiar votos [14, 15, 16, 17]. No queda claro si tal tipo de ataque ha sido montado contra Vot.ar.

En Holanda el voto electrónico dejó de usarse en 2007 al probarse que los votos podían ser leídos (en algunas máquinas) a varios metros de distancia y que los programas podían ser alterados (en las otras máquinas) [18].

En la India investigadores mostraron que es posible alterar las máquinas de votación con anterioridad a la elección y controlar los resultados mediante un dispositivo móvil [19].

En Irlanda evaluaron un sistema en elecciones piloto y determinaron que no se podía garantizar la integridad de ninguna elección que usara ese sistema. Los equipos fueron finalmente descartados, con un costo de más de 54 millones de euros [20, 21].

En 2007 tanto en California como en Ohio se les quitó la certificación a todas las máquinas de votación electrónicas por considerarlas inseguras [22, 23, 24]. Según la Secretaria de Estado de Ohio *"no system used in Ohio is without significant and serious risks to voting integrity"* [25].

Además de estos problemas inherentes a su naturaleza como programas, los sistemas de voto electrónico tienen una gran desventaja comparados con el voto tradicional por el problema de la *escalabilidad de las amenazas*: En un sistema tradicional, para crear cambios a una escala suficiente para cambiar una elección deben estar involucrados muchos individuos. En un sistema de voto electrónico, los individuos necesarios son muchos menos, y un par de líneas de código hábilmente ocultas pueden cambiar cientos de miles de votos.

Si se acepta que va a haber errores, se pueden tratar de implementar mecanismos que limiten el daño causado por un problema en el software. Un ejemplo de esta actitud es el concepto de *Software*

Independence[1] que Rivest y Wack adelantaron en 2006 y que luego fue publicado [26]. Lamentablemente muchos desarrolladores toman la actitud de que su producto no tiene errores, con lo cual sus productos resultan en realidad peligrosos ya que atacantes pueden utilizar estos errores para cambiar los resultados.

3.2. Problemas a nivel teórico. En cualquier sistema de votación debe garantizarse, entre otras cosas:

- El **secreto** del voto, lo que incluye la *no coercibilidad* del voto.
- La **fidelidad** del voto: el resultado final debe reflejar la voluntad de los electores.

Este último requerimiento suele subdividirse en los requerimientos de:

1. *integridad* del sistema: que el método propuesto para contar los votos los sume correctamente.
2. *verificabilidad* del sistema: que el sistema provea suficientes registros para poder saber si el resultado finalmente emitido coincide con el resultado teórico que debería haber producido el método propuesto en (1).

Los requerimientos de mantener el secreto pero al mismo tiempo poder corroborar la fidelidad del voto son contradictorios, puesto que para mantener el secreto no es deseable guardar mucha información sobre el voto en sí, con lo cual no es fácil hacer un sistema que permita ser auditado para comprobar si hubo o no algún problema.

Esto lo diferencia de por ejemplo un cajero automático, donde la identidad del extractor de dinero es conocida, y las transacciones quedan registradas. Aquí la identidad del votante debe ser oculta, para garantizar el secreto del voto.

Es un problema teórico interesante pero difícil de resolver. De hecho es imposible de hacer si queremos que los requerimientos se satisfagan de forma perfecta:

Teorema 1 (Teorema de Hosp y Vora [27])**.** *No existe ningún sistema de votación (electrónico o no) que tenga al mismo tiempo las propiedades de integridad perfecta, verificabilidad perfecta y privacidad perfecta.*

En vista a este teorema, declaraciones como “El sistema es 100 % seguro” (ONPE, en Perú [28, 29]), “El sistema no es vulnerable” (el presidente de MSA, sobre Vot.ar [30]) o “El sistema posee una invulnerabilidad...” (algunos periodistas sobre el sistema Vot-E de la UNCuyo [31]) son aventuradas e imposibles de demostrar.

De todos modos, aunque no se pueda lograr integridad, verificabilidad y privacidad perfectas, se puede intentar crear sistemas que se aproximen bastante a estos requerimientos. Algunos investigadores de InfoSec están trabajando en esta área, creando sistemas como Farnel [32], VoteHere [33], Prêt à

[1] Un sistema de votación electrónico es *software-independent* si un cambio no detectado en su software no puede producir un cambio no detectado en el resultado de la elección.

Voter [34], Punchscan [35], Scratch & Vote [36], ThreeBallot [37, 38], Scantegrity [39], Twin [38], Helios [40], etc. (no todos son de voto electrónico, algunos son mejoras en el sistema de papel, o en un sistema de conteo electrónico). Estos sistemas usan mucha criptografía, incluyendo cifrado de votos y *zero-knowledge-proofs*.

Pero existe un segundo problema teórico: el sistema debe ser **democrático**. No sirve de nada un sistema seguro, rápido, fidedigno, etc., si los únicos que lo pueden entender son miembros de una elite técnica. Pero por su naturaleza misma, eso es lo que suele pasar con los sistemas de Voto Electrónico. Esta fue una de las razones por las en el 2007 los sistemas de voto electrónico de tipo DRE usados hasta ese momento fueron declarados inconstitucionales en Alemania [41, 42].

Por lo tanto hay que agregar elementos que permitan al votante, aún sin entender todos los detalles, estar razonablemente seguro que las partes fundamentales del acto de votar se cumplen. Y este requerimiento no es fácil de satisfacer.

Entonces, ¿qué requerimientos deberíamos pedir a un sistema de voto electrónico, aún sabiendo que nunca tendremos seguridad perfecta? La idea básica es limitar las ventanas de ataque y reducir el daño causado por errores o malicia activa.

4. REQUERIMIENTOS

Requerimiento 1 (Reaseguro Individual)**.** El votante debe contar con la certeza de la confidencialidad de su voto. Es decir, de que la máquina que lo crea no puede revelarlo de ninguna forma. Esta seguridad debe ser una *seguridad del votante* en el momento de emisión del voto. No basta con afirmar "los expertos dijeron", "la auditoría fue buena", "el presidente de la compañía asegura", etc.

Se debe pensar que el votante y la máquina son adversarios, y darle al votante suficientes armas para derrotarla.

Requerimiento 2 (Transparencia)**.** El sistema debe ser lo más transparente posible.

- Debe evitarse cualquier sistema de VE que use Seguridad por Obscuridad [2].
- Se debe disponer de tiempo suficiente para que expertos de todo tipo, y no solo los designados por los partidos políticos, puedan estudiar el sistema. Dada la complejidad de un sistema de este tipo, el tiempo mínimo debe medirse en meses.
- El acceso al código debe ser abierto (*disclosed source software* [44]). Esto no implica que deba usarse una licencia de software libre, sino que el código debe estar disponible para su inspección por parte de cualquier ciudadano.

  Como consecuencia de este requerimiento no deben permitirse sistemas de código cerrado, en los cuales en el mejor de los casos el código es accesible sólo para un número reducido de expertos. Menos aún si luego no se permite documentar las vulnerabilidades.

[2] Si bien la seguridad por obscuridad puede considerarse como una capa válida, siempre que no sea la única, de un sistema, eso no es admisible en un sistema de voto democrático.

- Debe haber al menos una auditoría independiente del sistema completo, incluyendo el hardware, y sus resultados deben ser públicos. Dada las características de los sistemas de votación, esta auditoría debe ser *adversarial*[3].

Requerimiento 3 (Separación de Funciones)**.** El conteo electrónico debe ser realizado por una máquina físicamente distinta de la máquina que emitió los votos e incapaz de sobre-escribir electrónicamente los votos. En particular no deben permitirse los DREs, aún aquellos que producen registro en papel.

Requerimiento 4 (Capacidad de Auditoría no Electrónica)**.** El voto debe imprimirse en una boleta en forma legible por seres humanos. Esto permite, por un lado, que el votante verifique su voto, y por otro, permite realizar una auditoría de urnas elegidas al azar comparando el resultado del conteo electrónico con un conteo manual.

En una selección al azar de las urnas efectivamente usadas en la elección se realizará un conteo manual de los votos y se verificará que el conteo coincida con el conteo electrónico. Si este test falla más allá de un cierto umbral, el conteo electrónico de todas las urnas debe ser anulado, y se debe realizar el conteo de forma manual.

Requerimiento 5 (Independencia de la Identificación del Votante)**.** La identificación del votante debe realizarse en forma independiente del sistema de emisión de voto.
Deben estar prohibidos los sistemas que requieran la lectura de la huella digital, cualquier otro dato biométrico o la utilización de algún código individual para permitir usar la máquina de emisión de votos.

Requerimiento 6 (Homologación)**.** Debe existir un proceso de homologación, con una norma que los sistemas deben cumplir, y estos deben ser sometidos a verificación por parte de terceros para asegurar el cumplimiento de los requerimientos establecidos por dicha norma.

Requerimiento 7 (Autenticidad del Sistema)**.** Debe haber un mecanismo que garantice que el sistema a ser usado el día de la elección es auténtico e idéntico al que ha sido homologado.

4.1. Requerimientos de la Máquina Emisora del Voto.

Requerimiento 8 (No Persistencia)**.** La máquina que emite el voto no debe guardar ningún tipo de información sobre el voto o el votante. En consecuencia, nuevamente los DREs no deben se permitidos.

Requerimiento 9 (Protección Contra Lecturas no Autorizadas)**.** El sistema debe contar con una protección adecuada contra la lectura a distancia del voto. Esto incluye tanto la lectura del estado de los equipos[4], como del *token* o registro utilizado[5].

[3] Con esto queremos decir que la auditoría debe considerarse exitosa si encuentra errores.
[4] Por ejemplo, lectura de la pantalla captando sus radiaciones electromagnéticas (Van Eck Phreaking [43]).
[5] Si la boleta usa algún registro electrónico del voto, debe haber medidas de protección para evitar que el mismo pueda ser leído y registrado externamente.

4.2. Requerimientos de la Máquina que Cuenta los Votos.

Requerimiento 10 (Anonimización de las Boletas)**.** Las boletas no deben tener ninguna forma de identificación, como por ejemplo números en serie, que permita diferenciar una boleta de otra y permita saber quien votó a quien con el simple expediente de contar en que orden se votó o bien, debe haber un mecanismo de aleatoriedad en la distribución de las mismas, el cual debe quedar claro no sólo para las autoridades de mesa sino también para los votantes.

Requerimiento 11 (Resguardo de Claves)**.** En el caso de usar criptografía, se debe especificar cómo y quien se encargará de resguardar las claves criptográficas.

Además de estos requerimientos, se sugiere a nivel internacional que cualquier implementación del voto electrónico siga un camino de gradualidad y experiencias piloto antes de ser adoptado masivamente [5].

5. Conclusiones

Los mecanismos tradicionales de voto poseen una cantidad de problemas, lo que ha conducido a numerosas propuestas de sistemas de voto electrónico. Sin embargo, estos sistemas generan nuevos y diferentes problemas, sin que los problemas del voto tradicional necesariamente se subsanen. Esto implica que tenemos en realidad dos dimensiones de problemas, los del voto tradicional, a los que se agregan los del voto electrónico.

Nuestro aporte es proponer una serie de requerimientos que resultan imprescindibles en un sistema de votación electrónico, y estos parten de un enfoque que se basa en “desconfiar y verificar”.

Claramente resulta un problema abierto, y requiere el aporte de todos los sectores de la sociedad.

El voto es el derecho más básico de un ciudadano en una democracia, y por lo tanto es demasiado importante como para ser dejado en manos de un grupo de técnicos.

Referencias

[1] *Constitución de la Nación Argentina*, 1994, `http://infoleg.mecon.gov.ar/infolegInternet/anexos/0-4999/804/norma.htm`, obtenido el 28 de mayo de 2016.

[2] National Institute of Standards and Technology. *Developing an Analysis of Threats to Voting Systems: Preliminary Workshop Summary*, Maryland, 2005. `http://www.nist.gov/itl/vote/upload/threatworksummary.pdf`, obtenido el 29 de mayo de 2016.

[3] Brenda Struminger. *Fraude electoral: especialistas explican cómo se practica y cuánto influye en una elección*, Diario La Nación, 28 de agosto de 2015, `http://www.lanacion.com.ar/1822799`, obtenido el 29 de mayo de 2016.

[4] Shuki Bruck, David Jefferson, and Ronald L. Rivest. *A Modular Voting Architecture (“Frogs”).* Talk presented at WOTE 2001, reprinted in *Towards Trustworthy Elections: New Directions in Electronic Voting* (2010)

[5] `https://www.ndi.org/e-voting-guide/common-electronic-voting-and-counting-technologies`, obtenido el 28 de mayo de 2016.

[6] Ka-Ping Yee. *Building Reliable Voting Machine Software* , PhD thesis, University of California, Berkeley, 2007

[7] Douglas W. Jones. *Kazakhstan: The Sailau E-Voting System* in Direct Democracy: Progress and Pitfalls of Election Technology, IFES Election Technology Series,2010

[8] Philip Meyer. *Glitch led to 'Bush wins' call*, USA Today, 29 de noviembre de 2000, `http://www.unc.edu/~pmeyer/usat29nov2000.html`, obtenido el 28 de mayo de 2016.

[9] Grant Gross. *Voting machine glitch shows thousands of extra votes*, 2013, `http://www.networkworld.com/article/2328396/software/voting-machine-glitch-shows-thousands-of-extra-votes.html`, obtenido el 28 de mayo de 2016.

[10] Bruce Schneier. *An Incredibly Insecure Voting Machine*, `https://www.schneier.com/blog/archives/2015/04/an_incredibly_i.html`, obtenido el 28 de mayo de 2016.

[11] Diego Aranha. *Software vulnerabilities in the Brazilian voting machine*, publicado en Design, Development, and Use of Secure Electronic Voting Systems (2014) y tambien en RealWorldCrypto2016. `http://www.realworldcrypto.com/rwc2016/program`, obtenido el 28 de mayo de 2016.

[12] S. Amato, I. Barrera Oro, E. Chaparro, S. D. Lerner, A. Ortega, J. Rizzo, F. Russ, J. Smaldone, N. Waisman. *Vot.Ar: Una mala elección*, julio 2015. `https://github.com/HacKanCuBa/informe-votar/blob/master/Informe/informe.md`, obtenido el 28 de mayo de 2016.

[13] Enrique Chaparro. *El sistema de voto electrónico de la Ciudad de Buenos Aires: Una "solución" en busca de problemas*, Buenos Aires, 19 de junio de 2015, `http://www.vialibre.org.ar/wp-content/uploads/2015/06/VE.CdBuenosAires.Parte1_.pdf`, obtenido del 2 de junio de 2016

[14] Y. Oren y A. Wool. *Relay attacks on RFID-based electronic voting systems*. Cryptology ePrint Archive, Report 2009/442 (2009) `https://eprint.iacr.org/2009/422.pdf`, obtenido el 2 de junio de 2016.

[15] G.P. Hancke, K.E. Mayes y K.Markantonakis *Confidence in Smart Token Proximity: Relay Attacks Revisited* Elsevier Computers & Security, Vol. 28, Issue 7, pp 615-627. Octubre de 2009.

[16] Z. Kfir y A. Wool. *Picking virtual pockets using relay attacks on contactless smartcards*. En International Conference on Security and Privacy for Emerging Areas in Communications Networks, pages 47–58, Los Alamitos, CA, USA, 2005. IEEE Computer Society.

[17] I. Kirschenbaum and A. Wool. *How to build a low-cost, extended-range RFID skimmer*. En Proceedings of the 15th USENIX Security Symposium, Vancouver, B.C., Canada, 2006. USENIX Association.

[18] R. Gonggrijp y W.J. Hengeveld. *Studying the Nedap/Groenendaal ES3B voting computer: A computer security perspective*. En Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07), Boston, 2007.

[19] S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati, y R. Gonggrijp. *Security analysis of India's electronic voting machines*, en Proceedings of the 17th ACM conference on Computer and communications security, 2010, pp. 1–14. `https://indiaevm.org/evm_tr2010-jul29.pdf`, obtenido el 28 de mayo de 2016.

[20] Marie O'Halloran y Michael O'Regan. *E-voting machines to be disposed of*, The Irish Times, 6 de octubre de 2010, `http://www.irishtimes.com/news/e-voting-machines-to-be-disposed-of-1.865193`, obtenido el 29 de mayo de 2016.

[21] *Eliminated: After ten years and €55m, e-voting machines finally disposed of*, TheJournal.ie, 28 de junio de 2012, `http://www.thejournal.ie/e-voting-machines-disposed-phil-hogan-environment-fiasco-503678-Jun2012`, obtenido el 29 de mayo de 2016.

[22] Debra Bowen. *Top-to-Bottom Review*, 2007, California, `http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review`, obtenido el 28 de mayo de 2016.

[23] David Wagner. *Report on the California top-to-bottom review*, 2007, University of California, https://www.usenix.org/legacy/event/sec07/tech/wagner.pdf, obtenido el 28 de mayo de 2016.

[24] Patrick McDaniel, Matt Blaze, Giovanni Vigna et al. *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing*, 2007, Secretary of State of Ohio.

[25] Jennifer L. Brunner. *Project Everest Report of Findings*, 2007, Ohio.

[26] Ronald L. Rivest. *On the notion of 'software independence' in voting systems.* Philosophical Transactions of The Royal Society A 366,1881 (2008) p. 3759-3767.

[27] Hosp, Ben, y Poorvi L. Vora. *An information-theoretic model of voting systems*. Mathematical and Computer Modelling 48 (9),2008, p. 1628-45

[28] *Jefe de ONPE: "El voto electrónico es 100 % confiable"*, El Comercio, 1 de abril de 2016, http://elcomercio.pe/politica/elecciones/jefe-onpe-voto-electronico-100-confiable-noticia-1890976, obtenido el 2 de junio de 2016

[29] *ONPE: voto electrónico es 100 % confiable y de manejo sencillo*, Andina Agencia Peruana de Noticias, 1 de abril de 2016, http://www.andina.com.pe/agencia/noticia-onpe-voto-electronico-es-100-confiable-y-manejo-sencillo-605864.aspx, obtenido el 2 de junio de 2016

[30] Sergio Angelini. Programa "Lanata Sin Filtro", Radio Mitre, 11 de mayo de 2015. https://www.youtube.com/watch?v=8XdturQxK8Q, obtenido el 29 de mayo de 2016.

[31] *Es un paso: la UNCuyo pone en marcha el voto electrónico*, Mendoza Online, 19 de marzo de 2016, http://www.mdzol.com/nota/662673, obtenido el 2 de junio de 2016

[32] Ricardo Custódio. *Farnel: um protocolo de votação papel com verificabilidade parcial.* Invited Talk to Simpósio Segurança em Informática (SSI), Noviembre de 2001

[33] C. Andrew Neff y Jim Adler. *Verifiable e-Voting - Indisputable electronic elections at polling places*, 2003. http://media.eurekalert.org/aaasnewsroom/2004/2Neff-Verifiable-e-Voting-Paper.pdf, obtenido el 29 de mayo de 2016.

[34] P.Y.A. Ryan, P.Y.A. D. Bismark, J. Heather, S. Schneider y Z. Xia. *The Prêt à Voter Verifiable Election System*. IEEE Transactions on Information Forensics and Security 4 (4), 2009, p. 662–673

[35] K. Fisher, R. Carback and A.T. Sherman. *Punchscan: introduction and system definition of a high-integrity election system*. Proceedings of Workshop on Trustworthy Elections, 2006

[36] Ben Adida y Ronald Rivest. *Scratch & Vote - Self-Contained Paper-Based Cryptographic Voting*, 2006, https://people.csail.mit.edu/rivest/pubs/AR06.pdf obtenido el 29 de mayo de 2016.

[37] Ronald Rivest. *The Three Ballot Voting System*, 2006, http://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf, obtenido el 29 de mayo de 2016.

[38] Ronald Rivest y Warren Smith. *Three voting protocols: ThreeBallot, VAV, and Twin*, Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology, 2007, p. 16. https://people.csail.mit.edu/rivest/RivestSmith-ThreeVotingProtocolsThreeBallotVAVAndTwin.pdf, obtenido el 29 de mayo de 2016.

[39] David Chaum, Aleks Essex, Richard T. Carback III, Jeremy Clark, Stefan Popoveniuc, Alan T. Sherman y Poorvi Vora. *Scantegrity: End-to-End Voter Verifiable Optical-Scan Voting*, IEEE Security & Privacy (6:3), 2008, p. 40–46.

[40] Ben Adida. *Helios: web-based open-audit voting*, Proceedings of the 17th Conference on Security Symposium, San Jose, CA, 2008, https://www.usenix.org/legacy/events/sec08/tech/full_papers/adida/adida.pdf

[41] Bundesverfassungsgericht. *Leitsätze zum Urteil des Zweiten Senats vom 3. März 2009 – 2 BvC 3/07, 2 BvC 4/07*. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2009/03/cs20090303_2bvc000307.html

[42] Manfred Koessl, José M. Pérez Corti. *Inconstitucionalidad del E-Vote en Alemania - 2009, Parte I - Parte II*. Traducción y comentario a la Sentencia del Tribunal Constitucional Alemán, 2009.

[43] Wim van Eck. *Electromagnetic radiation from video display units: an eavesdropping risk?*, Computers and Security, Volume 4 Issue 4, Dic. 1985, p. 269 - 286.

[44] Dan Wallach. *On open source vs. disclosed source voting systems*, https://freedom-to-tinker.com/blog/dwallach/open-source-vs-disclosed-source-voting-systems

LICENCIA