# CONSIDERACIONES SOBRE EL VOTO ELECTRÓNICO

MIGUEL MONTES[1], DANIEL PENAZZI[2], AND NICOLAS WOLOVICK[3]

Abstract. Este trabajo es una breve exposición sobre el Voto Electrónico: sus posibles definiciones, debilidades, algunas experiencias en el mundo, y posibles requerimientos que un sistema de tal tipo debería satisfacer.

## 1. Introducción

En el proceso de votación, central al sistema electoral, pueden distinguirse tres etapas:

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

**Registro:** el voto es resguardado junto con otros votos de forma de anonimizarlo.

**Conteo:** luego de agotado el lapso disponible para votar, se cuentan los votos resguardados.

**Definición 1.** Una definición posible es llamar **"Voto Electrónico"** a cualquier sistema que introduzca computadoras en **alguna** de esas etapas Otra definición mas reducida es llamar "voto electrónico" a sistemas en donde la **emisión** y el **registro** del voto son electrónicos y "conteo electrónico" si las computadoras sólo se usan en el conteo.

1.1. **DREs e IREs.** En algunos sistemas de Voto Electrónico tanto la emisión como el conteo de votos se hacen en la misma máquina. A estos se los denomina generalmente DRE (*Direct Recording Electronic*),[1] y también suele llamárselos "urna electrónica". Algunos de ellos proporcionan un registro en papel que es guardado para posterior auditoría; a estos últimos se los denomina VVPAT (*Voter-Verified Paper Audit Trail*).[2]

Otros sistemas usan, aunque a veces de manera incompleta o incorrectamente implementada, la idea de [10] y separan físicamente la emisión del voto de su conteo: el elector crea un objeto físico en el que se registra su voto (un *token* o "boleta"), que es depositado en una urna para ser posteriormente contado, ya sea en forma manual o electrónica. Estos suelen ser llamados *Electronic Ballot Printers* (EBP)[18, 25] o *Indirect-Recording Electronic* voting machines (IRE).[15]

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 entregandosela 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 extras que no permitan reconstruir los votos individuales a partir de los registros internos de la máquina, pero el votante no puede verificar por si 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 mescla 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 mas séguros 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".[3]

Es un detalle que no vale la pena discutir mucho ahora, pero *en una ley de voto electrónico debería quedar claro cual definición de voto electrónico se usa*. Ademas, hay que tener cuidado en una ley en no especificar que se requiere un sistema de "Boleta Unica Electrónica", pues al parecer se trata de un término de denominación comercial, con lo cual se corre el riesgo de excluir cualquier competencia.

## 2. Problemas con el Voto Electrónico

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

2.1. **Problemas a nivel práctico.** Cualquier programa complejo tendrá inevitablemente bugs, incluyendo programas hechos por empresas como Apple, Microsoft o Bethesda. Si bien los sistemas producidos por estas empresas son mucho mas complejos que los sistemas de Voto Electrónico, los errores del código son sólo eso: errores. 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 mas electores.
- Se cuentan múltiples votos para un mismo candidato.
- 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.

Algunos ejemplos destacados:

- El ejemplo mas destacado es por supuesto en Volusia County, Florida, en el 2000: Gore recibió -16.022 votos (votos negativos). 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, sobre 50.000 votantes registrados, el equipo electrónico contó 140.000 votos.
- Mas recientemente en 2015 se descubió que el sistema AVS WinVote:
  - Tiene password débiles que no pueden ser cambiadas
  - Usa Wired Equivalent Privacy (WEP) (mostrado inseguro en 2001 y reemplazado por WPA desde 2003).
  - Usa una versión de Windows XP Embedded que no ha sido parchada desde 2004.
- El sistema usado en Brasil fue analizado en [7] encontrando entre otras las siguientes fallas:
  - Falla en la protección del secreto del voto:
    - 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.
    - El sistema de verificación de identidad del votante esta enlazado con la máquina de votación.
  - Uso de algoritmos criptográficos obsoletos.
  - Vulnerables a amenazas internas.
  - Falla en el uso de mecanismos de encriptación.
- Al sistema Vot.Ar se le encontraron entre otras las siguientes fallas:[6]
  - Las boletas pueden ser individualizadas.
  - El voto puede ser leído por un celular llevado por el votante con solo acercar el celular a la boleta, permitiendo la compra de votos.
  - Se puede generar una boleta que contenga mas de un voto.
- En Holanda el voto electrónico dejó de usarse en 2007 al probarse que los votos podian ser leidos a varios metros de distancia (en algunas máquinas), y que en las restantes los programas podían ser alterados.[12]
- En la India, cuyas máquinas son por diseño críticamente vulnerables a amenazas internas, se detectaron fallas serias a pesar de la "seguridad por oscuridad".[24]
- En Irlanda se adquirió un sistema; evaluaciones determinaron que no se podía garantizar la integridad de ninguna elección que lo usara. El costo del experimento fue 54 millones de euros, sin contar el gasto adicional para deshacerse de las máquinas jamás utilizadas, diez años después.[17]
- En 2007, tanto California como Ohio descertificaron todas las maquinas de votación electrónicas por considerarse inseguras. ("no system used in Ohio is without significant and serious risks to voting integrity"(Secretario de Estado de Ohio).

Ademas de estos problemas inherentes a su naturaleza como programas, los sistemas de voto electrónico tienen una gran desventaja frente al voto tradicional por el problema de la *escalabilidad de las amenazas*: En un sistema tradicional, para crear cambios a una escala suficiente para alterar el resultado de una elección deben estar involucrados muchos individuos. En un sistema de voto electrónico, los individuos necesarios son mucho 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" que Rivest y Wack adelantaron en 2006 y luego fue publicado por el primero en [20]. (Un sistema de votación electrónico es *software-independent* si un cambio indetectado en su software no puede producir un cambio indetectado en el resultado de la elección). Lamentablemente muchos desarrolladores toman la actitud de que su producto no tiene errores, con lo cual sus productos son muy peligrosos.

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

- El **secreto** del voto. (Esto incluye la *no coercibilidad* del voto.)
- La **fidelidad** del voto (el resultado final debe reflejar la voluntad de los electores)

Este último requerimiento suele divirse en los requerimientos de:

(1) *integridad* del sistema: que el método propuesto para contar los votos los cuente correctamente.
(2) *verificabilidad* del sistema: que el sistema provea suficientes registros como 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 si, con lo cual **no es fácil hacer un sistema que permita ser auditado** para comprobar si hubo o no algún problema.

Esto lo diferencia, por ejemplo, de un cajero automático, donde la identidad del extractor de dinero es conocida, y las transacciones quedan registradas. Aquí la identidad del votante no debe registrarse, a fin de garantizar el secreto del voto.

Es un problema teórico muy interesante pero muy difícil de resolver. De hecho es imposible de hacer si queremos que los requerimientos se satisfagan de forma perfecta. (Teorema de Hosp y Vora,[14]):

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

por lo cual declaraciones como "El sistema es 100% seguro" (ONPE, en Perú). "El sistema no es vulnerable" (el presidente de MSA, sobre Vot.Ar) o "El sistema posee una invulnerabilidad..." (creadores del sistema Vot-E de la UNCuyo) no son muy creibles.

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 serios están trabajando

en esta area, creando sistemas como Farnel,Vote Here, Pret A Voter, Punchscan, Scratch-and-Vote, ThreeBallot, Scantegrity, Twin, Helios, 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 encriptamiento de votos y *zero-knowledge-proofs*.

Pero, tenemos un segundo problema teórico con el voto electrónico: 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 el VE. Esta fue una de las razones por las en el 2009 los sistemas de voto electrónico usados hasta ese momento fueron declarados inconstitucionales en Alemania.[9] Citerios similares emplearon las cortes de Austria [23] y Finlandia [16].

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 esto no es fácil de hacer.

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.

## 3. Requerimientos

**Requerimiento 1. Requerimiento Fundamental:** El votante debe poder estar seguro de que la máquina que crea el voto, no lo revela individualizándolo de alguna forma.

Esta seguridad debe ser una seguridad **DEL VOTANTE** en el momento de emisión del voto y no que "*los expertos dijeron*", "*la auditoría fue buena*", "*el presidente de la compañía asegura*", etc.

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

**Requerimiento 2.** La máquina que emite el voto **no debe guardar ningún tipo de información** sobre el voto o el votante. En particular, DREs no deben ser permitidos, aún aquellos que producen registro en papel.

**Requerimiento 3.** El voto debe imprimirse en forma legible por humanos en la boleta.

En una selección al azar estadísticamente significativa 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 mas allá de un cierto umbral, el conteo electrónico de todas las urnas debe ser anulado, y se debe realizar el conteo manual de ellas.

**Requerimiento 4. Transparencia:** El sistema debe ser lo mas transparente posible.

- Cualquier sistema de VE que use "**Seguridad por obscuridad**" debe ser **evitado**.

- Se debe disponer de **amplio tiempo** (semanas, como mínimo, meses preferentemente) para que expertos de todo tipo (y no solo los "expertos designados por los partidos políticos") puedan **estudiar el sistema**.
- El **acceso al código** debe ser lo mas **abierto** posible. Muchos expertos consideran que es necesario que sea "open source software" o al menos "disclosed source software". Si esto no es posible, los *non-disclosure agreements* deben ser tales que los expertos puedan reportar las fallas que encontraron.[4]
- Sistemas de código cerrado y en los cuales las empresas sólo permiten verlo por un par de horas a un número reducido de expertos no deben ser permitidos. Menos aún si luego no se permite documentar las vulnerabilidades.
- Debe haber al menos una auditoría independiente realizada por profesionales calificados del sistema completo, incluyendo el hardware, y sus resultados deben ser públicos.

**Requerimiento 5.** El conteo electrónico debe ser realizado por una máquina físicamente distinta de la máquina que emitió los votos e incapaz de sobreescribir electrónicamente los votos.

**Requerimiento 6.** La **identificación** del votante debe realizarse en forma **independiente del sistema de emisión de voto**.

Sistemas que requieran la lectura de la **huella digital** o introducir algún código individual para permitir usar la máquina de emisión de votos deben estar **prohibidos**.

**Requerimiento 7.** El sistema debe contar con una protección adecuada contra emisiones captables a distancia, incluyendo la radiación electromagnética de pantalla,[22] las lumínicas,[8], audio,[21], radiofrecuencia[11] y otras señales explotables a distancia, dependiendo de los medios usados. Si la boleta usa algún registro electrónico del voto, debe haber medidas de protección para evitar que el mismo pueda ser leido y registrado externamente en forma no autorizada.[19, 13]

**Requerimiento 8.** Las boletas no deben tener ninguna forma de identificación (como 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 aleatoridad en la distribución de las mismas, el cual debe quedar claro no sólo para las autoridades de mesa sino también para los votantes.

**Requerimiento 9.** En el caso de usar criptografía, se debe especificar cómo y quien se encargará de resguardar las claves criptográficas.

**Requerimiento 10.** Se realizará una selección al azar de las máquinas de votación el dia de la elección para ser testeadas frente a téstigos, en una elección simulada en la cual todos los votos queden registrados en forma independiente y luego los resultados verificados. Esto sirve para detectar errores, pero no malicia activa, pues podría haber código que detecte si la máquina esta siendo usada para testeo o no.[5] Es una medida extra de seguridad, pero no es suficiente por sí sola.

No tiene ningún sentido realizar una auditoría previa del sistema mas revisión del código y la estructura general del mismo si luego no hay garantías que el sistema usado el día de la elección es el mismo que se revisó. Por lo tanto:

**Requerimiento 11.** Debe haber un mecanismo de autenticación del sistema completo a ser usado el dia de la elección, que asegure que cada sistema instalado es absolutamente idéntico a los testeados.

Ademas de estos requerimientos, se sugiere a nivel internacional (e.g., [18]) que cualquier implementación del voto electrónico siga un **camino de gradualidad** y experiencias pilotos antes de ser adoptado masivamente.

## References


[1] La denominación no es consensual. Algunos autores, y algunos marcos jurídicos, entienden como DRE al sistema que registra las opciones del elector en cualquier elemento de memoria pasible de posterior lectura automatizada. Véase por ejemplo la legislación del estado de California.

[2] El concepto fue propuesto originalmente por R. Mercuri, "A Better Ballot Box?", *IEEE Spectrum*, 39 (28):46–50, oct. 2002.

[3] Esta taxonomía no es generalmente aceptada en la literatura científica ni jurídica, aunque suele emplearse en denominaciones comerciales.

[4] En 2008, el desaparecido fabricante de sistemas de voto electrónico Sequoia amenazó a los profesores Felten y Appel de la Universidad de Princeton con acciones legales por infracción de copyright si revelaban fallas en uno de sus modelos, cuyo análisis les había sido encomendado por el estado de New Jersey.

[5] Algunos de los problemas del "testeo paralelo" fueron analizados en R. E. Crane, A. M. Keller, A. Dechert, E. Cherlin, y D. Mertz, *A Deeper Look: Rebutting Shamos on e-Voting*, 2005. El reciente caso sobre el control de emisiones en los motores diesel Volkswagen muestra dramáticamente que es posible ocultar software que proporcione resultados fraudulentos solo bajo determinadas condiciones. Véase L. Mearian, 'A diesel whodunit: How software let VW cheat on emissions", *Computerworld*, 23 de septiembre 2015.

[6] 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. Disponible en: https://github.com/HacKanCuBa/informe-votar/blob/master/Informe/informe.md

[7] Diego F. Aranha, M. M. Karam, A. Miranda, y F. Scarel "Software vulnerabilities in the Brazilian voting machine", en D. Zissis y D. Lekkas, eds., *Design, Development, and Use of Secure Electronic Voting Systems* (2014).

[8] M. Backes, M. Durmüth, y D. Unruh, "Gespiegelt / Verräterische Reflexionen: Wie Brillengläser Geheimnisse verraten", *iX Magazin für Professionelle Informationstechnik* 5: 115–117, (2008)

[9] Bundesverfassungsgericht (Corte Constitucional Federal de Alemania). *Leitsätze zum Urteil des Zweiten Senats vom 3. März 2009 – 2 BvC 3/07, 2 BvC 4/07.* Sentencia del Segundo Senado del 3 de marzo de 2009.

[10] Shuki Bruck, David Jefferson, y Ronald L. Rivest. *A Modular Voting Architecture ("Frogs").* Conferencia presentada en WOTE 2001, reimpresa en *Towards Trustworthy Elections: New Directions in Electronic Voting* (2010)

[11] D. Genkin, I. Pipman, E. Tromer, y L. Pachmanov, "Stealing keys from PCs using a radio: cheap electromagnetic attacks on windowed exponentiation", Laboratory for Experimental Information Security, Tel Aviv University, Tel Aviv, Research Report, (feb. 2015).

[12] 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.

[13] G. Hancke, "Practical eavesdropping and skimming attacks on high-frequency RFID tokens", *Journal of Computer Security* 19 (2): 259–288, (2011).
[14] Ben Hosp y Poorvi L. Vora. "An information-theoretic model of voting systems". *Mathematical and Computer Modelling* 48 (9): 1628-45 (2008)
[15] Douglas W. Jones; "Kazakhstan: The Sailau E-Voting System" en M. Yard, ed., *Direct Democracy: Progress and Pitfalls of Election Technology*, Washington, DC: International Foundation for Electoral Systems (IFES) (2010)
[16] Korkein hallinto-oikeus (Supremo Tribunal Administrativo de Finlandia), caso 9.4.2009/899 KHO:2009:39, sentencia del 9 de abril de 2009)
[17] R. McDermott, "Ireland: A Decade of Electronic Voting", en M. Yard, ed., *Direct Democracy: Progress and Pitfalls of Election Technology*, Washington, DC: International Foundation for Electoral Systems (IFES), (2010), pp. 96–107.
[18] https://www.ndi.org/e-voting-guide/common-electronic-voting-and-counting-technologies
[19] Y. Oren y A. Wool, "Attacks on RFID-Based Electronic Voting Systems", IACR Cryptology ePrint Archive, 2009-422 (2009)
[20] Ronald L. Rivest. *On the notion of 'software independence' in voting systems.* Philosophical Transactions of The Royal Society A 366,1881 (2008) pp. 3759-3767.
[21] A. Shamir y E. Tromer, "Acoustic cryptanalysis: On nosy people and noisy machines", Eurocrypt 2004 Rump Session)
[22] W. van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?", *Computers & Security*, 4 (4): 269–286 (dic. 1985).
[23] Verfassungsgerichthof (Corte Constitucional de Austria), caso V 85-96-11/15. Sentencia del 13 de diciembre de 2011)
[24] 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.
[25] Ka-Ping Yee, *Building Reliable Voting Machine Software* , PhD thesis, University of California, Berkeley, Fall 2007

1:Universidad Nacional de Córdoba, Instituto Universitario Aeronáutico
*E-mail address*: mmontes@iua.edu.ar

2:CIEM-FaMAF, Universidad Nacional de Córdoba
*E-mail address*: penazzi@famaf.unc.edu.ar

3:FaMAF, Universidad Nacional de Córdoba
*E-mail address*: nicolasw@famaf.unc.edu.ar