Voto Electrónico, Vulnerabilidades y Soluciones para Evitar Ataques

Joel Leandro Nardi[1] y Rosa Rita Maenza[2]

[1] Universidad Tecnológica Nacional, Facultad Regional Rosario.
Zeballos 1451, Rosario, Santa Fe. jnardi@frro.utn.edu.ar
[2] Departamento de Ingeniería en Sistemas de Información,
Universidad Tecnológica Nacional, Facultad Regional Rosario.
Zeballos 1451, Rosario, Santa Fe. rmaenza@gmail.com

Resumen. El presente trabajo se focaliza en la investigación y recopilación de vulnerabilidades informáticas observadas en algunas implementaciones de sistemas de voto electrónico. Se mencionan propuestas académicas desarrolladas sobre la temática en cuestión y se analizan diferentes formas de contrarrestar los puntos débiles detectados. Se describen protocolos empleando técnicas criptográficas que procuran resistir las diversas posibilidades de ataque. Finalmente se propone una solución que minimice la probabilidad de vulnerabilidad de un sistema de voto electrónico.

1 Introducción

La modernización del estado y en particular el mayor uso de tecnologías de la información y la comunicación en diversos estamentos de la sociedad ha determinado cambios importantes respecto a las formas de trabajo de organizaciones públicas y privadas.

En particular, la automatización e informatización del proceso electoral es uno de los puntos en que los gobiernos se han enfocado [1] [2]. El objetivo fundamental perseguido es lograr una mejor participación de la ciudadanía en pos de cubrir uno de los pilares del gobierno abierto [3].

Al hablar de voto electrónico nos estamos refiriendo a dos conceptos. Por un lado, el voto, como mecanismo mediante el cual los ciudadanos conviviendo en una democracia representativa, eligen a sus representantes. Por otro lado, el adjetivo de electrónico vinculado directamente al uso de la tecnología informática. Se trata entonces de un sistema de información en donde particularmente el valor de los datos adquiere una importancia vital vinculada a la democracia y los derechos ciudadanos.

En tal sentido, en materia de voto electrónico, es importante resaltar por lo menos tres categorías conceptual y tecnológicamente distintas: la lectura automatizada de votación en papel, la votación en medio electrónico autónomo y la votación electrónica en red [4].

Teniendo en cuenta estas diferencias, experiencias variadas se focalizaron en la realización de un escrutinio más rápido, garantizar la transparencia en el proceso electoral y en la adaptación del acto cívico de la votación preservando las condiciones de constitucionalidad.

Fundamentalmente el presente trabajo se focaliza en analizar la seguridad de los sistemas informáticos en las diferentes fases del proceso de implementación.

2 Antecedentes sobre implementaciones

Existen variadas implementaciones de sistemas de voto electrónico realizadas a nivel mundial con resultados diversos [5].

En particular, en Alemania se implementó un sistema en 2005, pero en 2009 se declaró inconstitucional, ya que según el máximo tribunal electoral de ese país, no había forma de que cualquier ciudadano sin conocimientos técnicos pudiese auditar la forma de votación [6] [7]. Otros países europeos llevaron adelante experiencias similares, retrocediendo posteriormente en su implementación, a considerar los casos de Holanda, Finlandia, Irlanda y Reino Unido. El caso de Irlanda tuvo como causa el presupuesto elevado que demandaba la implementación del sistema y la poca confianza que tenían los electores al momento de votar. En cuanto al caso holandés, se efectuaron estudios donde pudo observarse las graves fallas de seguridad que presentaba el sistema, generando mucha controversia y finalmente resultando en la negativa para seguir usando este método [8].

En Argentina, existe aún un debate controversial respecto al uso de esta tecnología. Si bien en el año 2006 se comenzó a tratar el tema en el Congreso Nacional, no se ha avanzado en un consenso general, solamente se realizaron algunas experiencias aisladas.

Una de ellas es la llevada a cabo en el año 2015 en las ciudades de Buenos Aires y Salta, donde se empleó el sistema de voto electrónico denominado Boleta Única Electrónica (BUE), desarrollado por la empresa Magic Software Argentina (MSA).

En dicha oportunidad, se resaltó como experiencia positiva la celeridad en la obtención de resultados, pero como contrapartida fueron detectadas fallas de seguridad importantes. En especial un experto en informática llamado Joaquín Sorianello, pudo realizar un ataque al sistema BUE dando a conocer el hecho y notificando a los desarrolladores [7].

Actualmente, hay otras provincias que intentan avanzar en esta línea de trabajo, particularmente Córdoba se propone implementar en el año 2019 el voto electrónico para elegir Gobernador y Legisladores. En la mencionada provincia, las ciudades de La Falda y Marcos Juárez hicieron uso del voto electrónico, con resultados positivos sobre su empleo [9].

3 Requerimientos de seguridad

Todo sistema de voto electrónico presenta una serie de requerimientos [10] [11] que deben ser tenidos en cuenta. Particularmente en este trabajo se analiza el correspondiente a seguridad.

Según el teorema de Hosp y Vora, no existe ningún sistema de votación (electrónico o no) que tenga al mismo tiempo las propiedades de integridad perfecta, verificabilidad y privacidad perfecta [12]. Entendiendo por integridad perfecta a la nula posibilidad de alteración del sistema, en otras palabras, la capacidad de resistir cualquier intento malicioso de ser modificado.

Según este planteo pensar en un sistema que sea invulnerable parece ser una utopía, sin embargo es posible intentar tomar las consideraciones y recaudos necesarios para reducir al mínimo las probabilidades de recibir ataques.

En el artículo "Consideraciones sobre el voto electrónico" de Miguel Montes, Daniel Penazzi y Nicolás Wolovick [5], los autores consideran una serie de requisitos sobre el sistema en estudio. Se mencionan los siguientes requerimientos:

1. Reaseguro individual. La identidad del votante no debe ser revelada. La máquina que crea el voto no puede revelar al votante.

2. Transparencia. Debe evitarse que se use seguridad por oscuridad [13]. Es decir, el acceso al código debe ser abierto, pudiendo ser inspeccionado por cualquier ciudadano [14]. Expertos de todo tipo deben poder estudiar el sistema. Es fundamental la existencia de una auditoría independiente del sistema completo y sus resultados deben ser públicos.

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 realizar una sobre escritura electrónica de los mismos.

4. Capacidad de auditoría no electrónica. El voto debe imprimirse en una boleta en forma legible para seres humanos. Esto permite la verificación por parte del votante y también posibilita realizar una auditoría de urnas elegidas al azar comparando los resultados del conteo electrónico con un conteo manual.

5. Independencia de la identificación del votante. Se recomienda que la identificación del votante se realice en dispositivos independientes de las urnas electrónicas.

6. Homologación. Norma que los sistemas deben cumplir debiendo ser sometidos a verificación por parte de terceros para asegurar su cumplimiento.

7. Autenticidad del sistema. Debe haber un mecanismo que garantice que el sistema a ser usado es auténtico e idéntico al que ha sido homologado.

8. No persistencia. La máquina que emite el voto no debe guardar ningún tipo de información sobre el voto o el votante.

9. Protección contra lecturas no autorizadas. El sistema debe contar con una protección adecuada contra la lectura a distancia del voto, es decir, que la metodología de votación puede resistir un ataque efectuado desde un dispositivo remoto, ya sea de forma presencial o no.

10. Anonimización de las boletas. Las boletas no deben poder ser identificadas. Debe haber un mecanismo de aleatoriedad en la distribución de las mismas.

11. Resguardo de claves. En el caso de usar criptografía se debe especificar cómo y quién se encargará.

Por otra parte, en el trabajo "Modelos de evaluación para sistemas de voto electrónico" de Aristides Dasso y Ana Funes [15], realizan otro estudio de requerimientos en donde es posible mencionar los siguientes ítems:

1. Controles de seguridad para el acceso y los componentes críticos del sistema, los cuales pueden contener contadores de votos.

2. Control de las funciones del sistema esperando que sólo se ejecuten de manera prevista.

3. Uso de lógica de control del sistema para controlar precondiciones.

4. Empleo de seguridad ante posibles ataques al sistema y ante fallas del mismo.

5. Uso de seguridad compatible con las tareas administrativas de preparación, prueba y operación. Significa que todas las tareas del sistema estén protegidos con métodos seguros.

6. Contar con la capacidad de accesos restringidos teniendo en cuenta funciones individuales.

7. Efectuar una documentación de los procedimientos obligatorios de seguridad.

Mientras que en el trabajo de Kohno et al [16] se resumen, como requisitos prácticos, las siguientes propiedades fundamentales que deben cumplir los sistemas de voto electrónico:

1. Mantener en el anonimato la identidad del votante responsable de cada voto.

2. Poseer un mecanismo robusto de defensa contra ataques informáticos.

3. Exponer una interfaz de usuario sencilla y amigable que pueda ser utilizada por cualquier persona.

De los anteriores análisis de requerimientos se deduce que existe un factor clave repetitivo, que se corresponde directamente con dar relevancia a los mecanismos vinculados con el encriptado y a la correcta selección de los protocolos de seguridad.

Si bien lograr que el votante realice de forma correcta el empleo del sistema de votación es una parte significativa para la seguridad del sistema, la información que se genera en el acto electoral es vital y puede llegar a ser un eslabón sensible a ser vulnerado. Esta vulnerabilidad, transitivamente genera que la elección no cumpla con la totalidad de sus requerimientos (deviniendo en un acto inconstitucional).

4 Vulnerabilidades

Actualmente, en diferentes países se están realizando investigaciones, estudios y pruebas sobre los sistemas de voto electrónico, pero existen escasos detalles sobre el uso e implementación de los mismos. Sin dudas esto se relaciona con la reticencia de las entidades para hacer público el código fuente y las especificaciones técnicas de sus desarrollos [17].

En particular, un estudio realizado en Estados Unidos sobre los equipos AccuVote efectuando un repositorio de control de versiones correspondiente al sistema, descubrió problemas con la identificación de los votantes [16]. La votación se llevaba a cabo por tarjeta, la cual era requerida para registrarse y emitir el voto único, pero los usuarios podían fabricar sus propias tarjetas, con lo cual se permitía emitir una cantidad de votos distinta a la que corresponde, sin dejar rastros de haber realizado fraude. Además, los votantes podían acceder a funcionalidades protegidas, llegando a poder detener el proceso de votación inclusive. Un usuario con experiencia suficiente podría alterar completamente el funcionamiento del equipo modificando el código ejecutable.

Otros estudios exponen algunas vulnerabilidades en equipos TSx y TS6 de calificación graves [18], pero los defectos mencionados no corresponden al voto electrónico en sí, más bien pueden definirse como debilidades que surgen por la arquitectura propia del sistema, comprometiendo también a la integridad del voto.

Una debilidad frecuente en sistemas de voto electrónico se encuentra en los mecanismos de encriptación de datos, que suelen ser poco robustos. En el proceso de enviar y recibir datos que los clientes realizan contra el servidor central, presentan la vulnerabilidad de emplear técnicas de encriptado muy deficientes. Además, es muy frecuente que no se verifique la integridad del mensaje transmitido en esas interacciones.

En tal sentido, Karlof et al [19] expone dos protocolos criptográficos pensados especialmente para sistemas de voto electrónico, ya implementados por Votegrity y VoteHere. Los autores destacan una serie de consideraciones pensadas para:

a. Verificar que un voto se almacene correctamente.

b. Comprobar que el conteo es correcto.

c. Mantener la privacidad del voto.

d. Evitar coerción o venta de votos.

El sistema prevé que el votante cuente con un comprobante impreso el cual le permitirá verificar si su voto fue correctamente contado, pero no tiene forma de probar su intención de voto a otra persona.

Si analizamos el sistema BUE implementado en Argentina bajo las consignas definidas por Karlof, se puede apreciar que son cumplidas

Pero, pese a que los criterios de Karlof reducen las múltiples cuestiones a solucionar en el tema de vulnerabilidad, se siguen presentando problemas. En especial, cabe destacar que estas consideraciones fueron tenidas en cuenta en el sistema BUE implementado en Argentina, pero se mencionó anteriormente que igualmente fue vulnerado.

El sistema de la boleta electrónica (BUE) incluye un chip, que puede ser destruido, leído y modificado desde una distancia variable de 50 centímetros y posiblemente más. El chip está numerado, así que si el presidente de mesa o el sistema puede identificar el número de chip correspondiente a un votante, podrá identificar quién votó a quién.

Si bien las boletas tienen una banda magnética que pretende solucionar este problema, basta que no se doble lo suficiente a la boleta, o que quede un pequeño espacio de milímetros, para que pueda leerse el voto.

En este punto es importante mencionar otras formas de violar el secreto del voto tales como:

- El uso de ondas electromagnéticas.
- El empleo de ruido eléctrico.
- El almacenamiento de datos.

Con lo expuesto, se observa que los algoritmos de encriptado pueden ser sensibles a técnicas de criptoanálisis y ataques de fuerza bruta, por lo cual si son de poca robustez resultan vulnerables [20].

5 Soluciones propuestas

Para que un sistema de voto electrónico funcione de forma segura, deben cumplirse los siguientes objetivos:

- Autenticación. Solo los votantes identificados en el padrón pueden votar, acto que se realizará una única vez.
- Anonimato. Ningún voto realizado puede ser identificado de alguna forma con algún votante.
- Integridad de datos. Los datos al ser transportados deben mantener su integridad.

- Auditoría. El sistema debe ser completamente auditable en cualquier etapa del proceso.
- Confidencialidad, integridad y no-denegación del servicio. Implica garantizar respuesta de parte del sistema a ataques informáticos, resguardando los datos y cuidando la disponibilidad.
- Seguridad en la interfaz del usuario. Garantizar que la interfaz pueda ser utilizada por cualquier persona, esto implica tener consideraciones sobre casos de personas con diferentes capacidades.

Si bien se han considerado y analizado propuestas que en menor y mayor medida toman en consideración la seguridad de la información con protocolos o a nivel procedural [21] [22], estos trabajos no cumplen las expectativas como para formalizar una solución totalmente eficiente.

La autenticación de los votantes puede ser realizada de forma presencial o remota. Esto implica dos alternativas, forma electrónica local (base de datos en el equipo de las autoridades de mesa), o forma remota (base de datos en línea). El empleo de equipamiento electrónico para autenticar los datos de un votante constituye una mejora en la dinámica del acto electoral y una forma de reducir errores humanos en procesos de autenticación. Las posibilidades de reconocimiento de un votante son varias (tarjetas asignadas a votantes, lecturas biométricas, códigos de barras), pero es conveniente incluir una clave de seguridad, privada, encriptada con un algoritmo de cifrado asimétrico, preferentemente el algoritmo RSA antes que ElGamal, ya que éste último presenta mayor riesgo de ataques (evidencia susceptibilidad a ataques de texto plano, mientras que RSA solo es susceptible si se logra obtener la clave privada a partir de la clave pública [20]).

Para mantener el anonimato del votante, se recomienda resguardar el lugar donde se realice la votación, para evitar presencia de equipos de monitoreo o rastreo de señales que puedan resultar de amenaza al anonimato del voto emitido. A su vez se recomienda la independencia de equipos entre los de la mesa de autoridades electorales y el que se emplea para la votación.

La integridad de los datos no debe ser modificado. Para tal cuestión se considera elemental incorporar algoritmos de encriptado. Si bien en el análisis un algoritmo asimétrico puede llegar a ser más seguro que uno simétrico, dadas las condiciones del considerable flujo de datos que se presenta en las elecciones es recomendable optar por la segunda opción, con preferencia en el uso del algoritmo AES, considerado el más seguro y tomado como estándar [20].

Respecto a la arquitectura a utilizar, es importante proteger la disponibilidad e integridad del sistema permanentemente. En tal caso lo más recomendable es emplear sistema operativo y hardware diseñado a medida del sistema. Es decir, que los componentes de software y electrónicos, sean particularmente pensados y desarrollados para los requerimientos de este sistema en particular, evitando piezas o desarrollos genéricos. En la capa de transporte, el protocolo de mayor aceptación es SSL, que crea un canal cifrado y cuenta con tres subprotocolos (handshake, change cypher spec,

alert), y además es el que ha tenido mayor uso en sitios donde se manejan datos privados, por lo tanto su implementación es más que recomendable.

Todos los componentes deben ser auditables, incluyendo código fuente, diseño, protocolos de comunicación, algoritmos utilizados y mecanismos de encriptación entre otros. De ese modo se permite a los investigadores y ciudadanía en general revisar el sistema desde distintos puntos de vista.

6 Algunos resultados y observaciones

El análisis de cuestiones que exponen debilidades en el proceso (como pueden ser las lecturas a distancia) no son tenidos en cuenta en la obtención de resultados en sentido operativo. Es decir, se hizo hincapié sobre qué se puede realizar sobre los algoritmos de encriptado ya que su función incide sobre la protección de datos.

Considerando la implementación de soluciones propuestas podemos tener en cuenta que usar RSA, limita la probabilidad de ataque al mínimo ya que implica la necesidad de obtener la clave privada a partir de la pública a partir de n.

Se puede mejorar AES para aumentar su seguridad, aumentando el tamaño de la clave (Tabla 1), aunque no es académicamente aceptado ya que se busca mejorar los algoritmos desde el punto de vista conceptual y matemático. El empleo de claves grandes afecta de forma negativa al rendimiento de los algoritmos simétricos. Se recomienda utilizar algoritmos de encriptado asimétrico para proteger la clave.

Tabla 1. Longitud de clave simétrica vs permutaciones

Tamaño de clave en Bits	**Permutaciones**	**Tiempo para un ataque de fuerza bruta para un dispositivo que realiza 2^{56} permutaciones por segundo**
8	2^{8}	0,001ms
40	2^{40}	0,015ms
56	2^{56}	1s
64	2^{64}	4m 16s
128	2^{128}	149 745 258 842 898 años
256	2^{256}	50 955 671 114 250 072 156 962 268 275 658 377 807 020 642 877 435 085 años

7 Discusión

Es de vital importancia retomar palabras de expertos y tomar consciencia de que ningún sistema de voto electrónico puede resultar completamente seguro [7] [8] [12]. Muchas compañías aseguran haber llegado a desarrollar sistemas de voto electrónico sin vulnerabilidades, incluso afirmando que pueden sortear las posibilidades de ata-

ques. Los argumentos presentados en el presente trabajo, en cierto modo, refutan estas afirmaciones.

La discusión planteada a nivel político, muchas veces supera a la realidad que existe en el ámbito tecnológico. En este tipo de proyectos es crucial la incorporación de equipos técnicos que asesoren a quienes cumplen la función pública, explicando los riesgos reales que hoy en día existen.

Las prácticas recomendadas como soluciones podrían llegar a minimizar el riesgo de un ataque. Pero aun así, la probabilidad de sufrirlo es real aunque pueda ser reducida al mínimo. Las personas que promueven el voto electrónico deberían ser conscientes de esta situación para no generar falsas expectativas.

En trabajos posteriores a éste, se pretende focalizar el análisis en el intento de mejorar conceptual y matemáticamente los algoritmos de encriptado, logrando estándares más seguros que los actualmente empleados. Además se procurará poner en discusión el uso de los protocolos y las formas de encriptar los datos, analizando variantes de posible utilización.

8 Conclusión

Conceptualmente se puede concluir que incorporando las soluciones propuestas, cuidando el manejo de protocolos y algoritmos de cifrado (asimétricos y simétricos), se pueden reducir las posibilidades de sufrir ataques y aumentar considerablemente la confiabilidad en los sistemas de voto electrónico.

De todos modos, es fundamental advertir una realidad innegable hoy en día, no hay sistema que no tenga vulnerabilidades. Ciertamente, en un futuro inmediato los algoritmos de encriptado puedan seguir siendo mejorados, de forma tal de tender a erradicar este problema.

En particular, existen varios factores que pueden sumarse para justificar la desconfianza de la sociedad en la implementación de este tipo de aplicaciones informáticas. Por ejemplo, la imposibilidad de ser auditable por cualquier ciudadano, genera desconcierto entre las personas que no tienen conocimientos técnicos, pues no están en condiciones de inspeccionar plenamente al equipo que opera en cada mesa electoral.

Considerados algunos aspectos negativos, también es necesario analizar los puntos fuertes que tiene el sistema, la celeridad en obtener resultados, es fundamentalmente una importante mejora comparada con los tiempos que toma efectuar un recuento de forma manual.

Por último, es necesario hacer mención de una situación existente por sobre la temática abordada en el presente trabajo. La sociedad actual incorpora tecnología a las diversas actividades cotidianas, por lo que pese a la resistencia por parte de algunos sectores, este tipo de innovación tecnológica se terminará incorporando en el ámbito político.

La recomendación dada por los expertos tiene que ver con la forma paulatina de implementar estos tipos de procesos, pues de esa forma es posible analizar, evaluar y cotejar el impacto que puede tener el empleo de los mismos en la sociedad. Las personas, poco a poco, deberán aceptar esta novedosa forma de votar, y el sistema tendrá que ganarse la confianza del electorado siendo lo menos vulnerable como le sea posible.

Referencias

1. LATHROP, Daniel y LAUREL, Ruma. Open Government. Collaboration, Transparency, and Participation in Practice. Ediciones O´Reilly Media, 2010.
2. OSZLAK, O. y KAUFMAN, E. (2014). Teoría y práctica del gobierno abierto: Lecciones de la experiencia internacional. E-Book: IDRC-CRDI/Red GEALC/OEA.
3. KAUFMAN, E. (2004). Participación ciudadana y gestión pública: Modelo Asociativo de Gobierno Electrónico Local. En A. Ziccardi (Coord.). Participación ciudadana y políticas sociales en el espacio local. Instituto de Investigaciones Sociales/UNAM: México DF.
4. RAMÍREZ-ALUJAS, A. V., y GÜEMES, M. C. Gobierno Abierto, reforma del Estado y modernización de la gestión pública: alcances, obstáculos y perspectivas en clave latinoamericana. In A. HOFFMAN, A. V. RAMÍREZ-ALUJAS & J. A. BOHÓRQUEZ-PÉREZ NIETO (Eds.), La Promesa del Gobierno Abierto, México DF. 2012, pp. 193-224.
5. Miguel MONTES, Daniel PENAZZI, Nicolás WOLOVICK. Consideraciones sobre el voto electrónico. 45 JAIIO, 10º Simposio de Informática en el Estado, 2016. ISSN: 2451-7534, pp 297-307.
6. Ariel TORRES. Algunas reflexiones sobre el voto electrónico. Diario La Nación, 11 de julio de 2015.
7. Brenda STRUMINGER. Boleta Electrónica: expertos muestran cómo vulneran el secreto del voto. Diario La Nación, 21 de octubre de 2016.
8. Martín DINATALE. Mitos y verdades sobre el voto electrónico en el mundo. Diario La Nación, 5 de agosto de 2015.
9. Gabriela ORIGLIA. Córdoba aprobó la boleta electrónica para 2019. Diario La Nación, 22 de diciembre de 2016.
10. PESADO, Patricia Mabel; FEIERHERD, Guillermo Eugenio; PASINI, Ariel C. Especificación de requerimientos para sistemas de voto electrónico. En XI Congreso Argentino de Ciencias de la Computación. 2005.
11. FEIERHERD, Guillermo Eugenio, et al. Una aproximación a los requerimientos del software de voto electrónico de Argentina. En X Congreso Argentino de Ciencias de la Computación. 2004.
12. HOSP, Ben, y Poorvi L. VORA. An information-theoretic model of voting systems. Mathematical and Computer Modelling 48(9), 2008. pp 1628-1645.
13. National Institute of Standards and Technology. Developing an Analysis of Threats to Voting Systems: Preliminary Workshop Summary, Maryland, 2005.
14. Dan WALLACH. On open source vs. disclosed source voting systems. 16 de abril de 2009.
15. Aristides DASSO, Ana FUNES. Modelos de evaluación para sistemas de voto electrónico. Universidad Nacional de San Luis. Mayo de 2011.
16. T. KOHNO, A. STUBBLEFIELD et al. Analysis of an electronic voting system. IEEE Simposio sore Seguridad y Privacidad. Mayo de 2004.

17. Allan BERROCAL, Gabriela BARRANTES SLIESARIEVA. Consideraciones de seguridad para la implementación de un sistema de voto electrónico en Costa Rica. Universidad de Costa Rica, Escuela de Ciencias de la Computación e Informática, 2007.
18. H. HURSTI. Diebold TSx evaluation, security alert. Black Box Voting Consumer Protection for Elections. Renton, Washington, Mayo de 2006.
19. C. KARLOF, N. SASTRY, D. Wagner. Cryptographic voting protocols: a systems perspective. USENIX Security Simposium, 2005.
20. Federico PACHECO. Criptografía. Ed. Users. ISBN: 978-987-1949-35-9. 2014.
21. P. PESADO, A. PASINI, E. IBAÑEZ, N. GALDÁMEZ, F. CHICHIZOLA, I. RODRÍGUEZ, C. ESTREBOU, A. DE GIUSTI. E-government: el voto electrónico sobre internet. Instituto de Investigación en Informática, Universidad Nacional de La Plata. Octubre de 2008.
22. URDAY CHÁVEZ, Marco. Diseño e implementación de un equipo de voto electrónico. Universidad Católica del Perú. Lima, Noviembre de 2012.