Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Cs. Exactas e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Tema
Voto electrónico

Título
Desarrollo de sistemas de votación seguros utilizando tecnologías contemporáneas

Autor: Ing. Luis Marcelo Castro
Tutor del Trabajo Final: Dr. Juan Pedro Hecht

Año de presentación
2019
Cohorte del cursante
2016

Declaración Jurada del origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO
Luis Marcelo Castro
DNI 31.626.229

Resumen

Este trabajo aborda la problemática del uso de la tecnología en el diseño de sistemas de votación y su estado de situación.
Se presenta un marco teórico inicial con las propiedades que deben cumplirse para fortalecer la seguridad de la información y cómo los avances en la tecnología junto con el desarrollo de técnicas criptográficas posibilitan nuevos casos de estudio. El análisis comprende una recopilación de propuestas de implementación, mostrando puntos a favor y en contra de cada una de ellas. Para completar el panorama general también se consideran las líneas de investigación más innovadoras y se plantean escenarios para futuros trabajos.
Se concluye que los beneficios reales que ofrece el voto electrónico son limitados y, al menos hasta el momento, no son superiores a los riesgos a los que nos expone.

Palabras clave: voto electrónico, criptografía, privacidad, verificabilidad de extremo a extremo, auditorías

Índice de contenidos

Introducción 1

1. Sistemas de votación seguros 2

1.1. Privacidad 2

1.2. Integridad 2

1.3. Disponibilidad 2

1.4. Auditabilidad 2

1.5. Accesibilidad 3

1.6. Usabilidad 3

1.7. Robustez 3

1.8. No repudio 3

2. El voto electrónico 5

2.1. Ventajas 5

2.1.1. Transparencia 5

2.1.2. Rapidez y exactitud del conteo 5

2.1.3. Reducción de costos 6

2.1.4. Menor impacto ecológico 6

2.1.5. Agilidad y sencillez 6

2.1.6. Mayor participación ciudadana 6

2.1.7. Modernización 6

2.2. Problemas intrínsecos 6

2.2.1. Magnitud de los fallos 7

2.2.2. Necesidad de controlar el voto emitido 7

2.2.3. Mantenimiento y configuración de los dispositivos 7

2.2.4. Retrasos ante fallos 7

2.2.5. Imposibilidad de auditar 7

2.2.6. Pérdida de la privacidad 7

2.3. Vectores de ataque 8

2.3.1. Máquinas de votación hackeadas 8

2.3.2. Ataques a la red 8

2.3.3. Daños al hardware 8

2.3.3. Manipulación de resultados 8

2.3.5. Voto no autorizado 8
2.3.6. Voto múltiple 9
2.3.7. Coerción 9
3. Paradigmas para el diseño de sistemas electrónicos de votación 10
3.1. Independencia del software 10
3.2. Verificabilidad de extremo a extremo 10
3.3. Auditorías limitantes del riesgo 11
3.4. Privacidad eterna 11
4. Primitivas criptográficas 13
4.1. Esquema de Shamir (Shamir's Secret Sharing) 13
4.2. Firma grupal (Group signature) 13
4.3. Firma ciega (Blind signature) 14
4.4. Cifrado Homomórfico (Homomorphic encryption) 14
4.5. Permutación criptográfica (Cryptographic shuffling) 15
4.6. Cifrado de clave pública (Public key encryption) 15
4.7. Pruebas de conocimiento cero (Zero knowledge proofs) 16
4.8. Redes de mezclado (Mix-nets) 16
5. Implementaciones destacadas 18
5.1. Voto electrónico presencial (e-voting) 18
5.1.1. Scantegrity 18
5.1.2. Prêt à Voter 21
5.1.3. STAR-Vote 24
5.2. Voto electrónico remoto (i-voting) 26
5.2.1. Remotegrity 26
5.2.2. Helios 28
5.2.3. Civitas 31
6. Líneas de investigación actuales 35
6.1. Blockchain 35
6.1.1. Conceptos básicos de blockchain 35
6.1.2. Aplicación en sistemas de voto electrónico 35
6.2. Computación cuántica 36
6.2.1. Conceptos básicos de computación cuántica 37
6.2.2. Protocolos cuánticos para voto electrónico 37

7. Propuestas para trabajo a futuro 39
8. Conclusiones 40
9. Bibliografía 42

Introducción

Llevar adelante un proceso de elecciones comprende la intención de cumplir con las normas democráticas y proteger los intereses de los ciudadanos, quienes tienen el derecho y a la vez la obligación de elegir a sus representantes. No es suficiente entonces que una elección produzca el resultado correcto; el electorado también debe tener la tranquilidad y el convencimiento de que los resultados anunciados realmente cumplen con la voluntad popular.

El uso de la tecnología para hacer más eficientes los sistemas de votación se discute desde hace décadas en ámbitos jurídicos, políticos y académicos sin llegar a conclusiones terminantes.

El objetivo del presente trabajo final de especialización es brindar algo de claridad a una parte de la discusión, abordando la faceta técnica y los aspectos del voto electrónico que refieren a la seguridad de la información. Para tal fin se consultaron numerosas fuentes profesionales, artículos, investigaciones y desarrollos y se analizó dicha información para reflejar el estado del arte en la materia de la forma más simple y amena posible tanto para el público conocedor de la temática como para el lector sin conocimientos especializados.

A continuación, se sintetiza la estructura que presentará este trabajo:

En el capítulo 1 se hará una revisión de las propiedades esperadas, necesarias y deseables que un sistema de votación debe tener, expresadas como requerimientos no funcionales de un sistema informático. El concepto de voto electrónico, así como sus ventajas y puntos débiles serán expuestos a lo largo del capítulo 2. El capítulo 3 introducirá una serie de paradigmas sirven para orientar el desarrollo de sistemas electrónicos de votación en conjunto con el conjunto de técnicas criptográficas que se detallarán en el capítulo 4.

Las implementaciones actuales concretas, su descripción y análisis se podrán ver en el capítulo 5, mientras que en el capítulo 6 se abre la puerta a tecnologías disruptivas que tienen el potencial de revolucionar el futuro del voto electrónico.

El capítulo 7 estará destinado a exponer recomendaciones, propuestas e ideas para guiar futuras investigaciones y finalmente en el capítulo 8 se expondrán los pensamientos y las conclusiones que se ofrecen como aporte de esta obra.

Se espera que este documento pueda servir para su difusión y alcance la relevancia suficiente como para ser fuente de consulta de futuros trabajos.

1. Sistemas de votación seguros

Actualmente nos encontramos ante un gran número de sistemas de votación en todo el mundo, pero aún frente a esta variedad se reconocen una serie de condiciones que son necesarias para que un sistema de votación pueda ser considerado como confiable. También existen otras cualidades que aún sin ser indispensables sí son deseables.
Además, resulta interesante y de suma importancia evaluar el cumplimiento de los principios básicos de seguridad de la información en el contexto de estos procesos cruciales para el funcionamiento de un Estado democrático.

1.1. Privacidad

Una de las primeras características que se debe cumplir es el secreto de la opción seleccionada por cada votante. De esta forma se facilita la libre expresión de la voluntad de cada persona. Incluso también debería estar garantizado que sea imposible demostrar frente a terceros cuál fue el candidato elegido.
La libertad de voto implica impedir que alguien sea inducido a votar de determinada manera, ya sea a través de la compra de votos o mediante la intimidación. La persona que vota debe tener seguridad de que no hay manera de que su voto sea conocido por otros.
Tampoco debería ser posible emitir un voto en lugar de otra persona (suplantación de identidad) o evitar que alguien emita su voto.

1.2. Integridad

A medida que se reciben votos también será tarea del sistema de votación garantizar que los mismos no se pierdan ni se modifique su valor. Los votos deben ser registrados respetando la elección de cada votante para permitir que el conteo y los resultados sean fehacientes.

1.3. Disponibilidad

El sistema de votación debe estar en funcionamiento y disponible para toda aquella persona habilitada para votar durante todo el período previamente definido para la votación. También es importante evitar interrupciones en las etapas de conteo de votos y publicación de resultados, aunque en este caso cierta tolerancia podría ser debatible.

1.4. Auditabilidad

Se necesita que existan instancias de verificación del correcto funcionamiento del sistema. Tales verificaciones podrán ser llevadas adelante por diferentes grupos de

interesados: fiscales partidarios, autoridades judiciales, ciudadanos de a pie, etc. La auditabilidad ayuda a conseguir elecciones limpias y resultados no cuestionables.

1.5. Accesibilidad

El sistema tiene que contemplar que la forma de emisión de los votos sea adecuada para todas las personas habilitadas para votar. Nadie debe estar imposibilitado de participar de las elecciones dando su voto aún cuando se trate de personas con alguna incapacidad o ciudadanos de edad avanzada.

1.6. Usabilidad

Es valorable que la forma de votar sea sencilla y práctica, brindando al electorado una experiencia lo más agradable posible a fin de favorecer el porcentaje de participación en el proceso electoral. Es esperable que la gran mayoría de los votantes no sean expertos en informática (e incluso que un considerable porcentaje sean analfabetos tecnológicos) y aún así todos ellos deben poder emitir sus votos con facilidad.

1.7. Robustez

Con esta característica se hace referencia a que el sistema debe ser tolerante a eventuales fallos. Esto no quiere decir que el sistema esté excento de problemas, sino que sea capaz de afrontarlos y superarlos. Se valora la existencia de planes de contingencia adecuados.

1.8. No repudio

Debe haber registros sobre quién ha votado (no sobre cómo fue su voto). Ninguna persona que votó debería poder negar haberlo hecho y ninguna persona que no votó debería poder afirmar haberlo hecho.

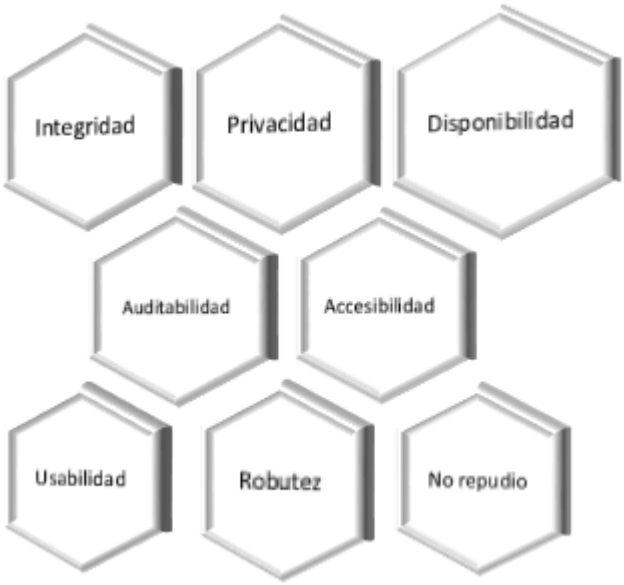

Imagen 1 - Propiedades de los sistemas de votación seguros. Fuente: Elaboración propia.

Algunas de las propiedades recién mencionadas están íntimamente relacionadas mientras que otras parecen ser contradictorias entre sí. En ese caso será un mérito del sistema de votación el decidir cuáles de ellas cumple y cómo armoniza los posibles conflictos.

Cabe destacar también que el listado de propiedades presentado en este trabajo está lejos de ser una versión definitiva y consensuada dentro del ámbito académico [2, 7, 26], pues también se trata de una línea de investigación que actualmente sigue activa.

2. El voto electrónico

Para presentar este concepto en primer lugar se debe aclarar que existe más de una interpretación del término “voto electrónico” [8].
En un principio, la introducción de tecnologías de la información en los procesos electorales tuvo como objetivo la automatización del escrutinio de los votos. Se desarrollaron entonces sistemas de reconocimiento óptico de marcas (OMR, por su sigla en inglés) para escanear las boletas y contabilizar la elección del ciudadano. Luego comenzaron a aparecer propuestas de índole tecnológica que contemplaban también el registro y la selección de los votos a través del registro electrónico directo (DRE) a través de dispositivos diseñados a tales efectos.
En el sentido más amplio de la expresión se define como voto electrónico a la utilización de dispositivos informáticos en cualquiera de las etapas del proceso de votación. Esto incluye la confección de los padrones, la emisión, guardado y conteo de los votos y publicación de resultados hasta las auditorías y chequeos.
En este trabajo se abordará puntualmente la intervención de computadoras en las instancias de emisión de los votos y en el recuento de los mismos en el lugar donde fueron recibidos.
También debe hacerse una distinción entre dos diferentes tipos de sistemas de voto electrónico: en primer lugar, se habla de sistemas de voto electrónico presenciales cuando los votantes concurren a lugares preestablecidos a emitir sus votos (e-voting), en contraste con los sistemas de voto electrónico remotos (i-voting o voto a través de internet).

2.1. Ventajas

La intención de que las elecciones utilicen dispositivos y mecanismos informáticos se argumenta en base a una serie de beneficios que la tecnología puede aportar. A continuación, se detallan y se analizan algunas de las ventajas más salientes de las propuestas a favor del voto electrónico.

2.1.1. Transparencia

En palabras de los impulsores del voto electrónico, la tecnología a utilizar permite la eliminación de prácticas fraudulentas como el robo de boletas y el voto en cadena.
Irónicamente esta sensación de transparencia se obtiene a costa de depositar la confianza del electorado en una virtual caja negra.

2.1.2. Rapidez y exactitud del conteo

Quizás este punto sea el más potente a analizar como ventaja. En el mejor de los casos se podría disponer de los resultados de la elección de forma casi instantánea a la finalización de los comicios. Esto suponiendo que no hubiera ningún tipo de falla o irregularidad.

2.1.3. Reducción de costos

A grandes rasgos la utilización de dispositivos electrónicos puede generar el ahorro no sólo los costos de la impresión y distribución de boletas sino también el almacenamiento de las urnas hasta los recuentos definitivos. Cuanto mayor sea la escala de la elección que se lleve a cabo más se acentúa la conveniencia de esta opción. Por otro lado, también hay que decir que se agrega la inversión en software y hardware, los costos de capacitación de personal, soporte técnico y reposición de equipos dañados.

2.1.4. Menor impacto ecológico

Algunos consideran que un sistema de voto electrónico tiene menor efecto ambiental, dada la utilización y desperdicio de papel en las boletas partidarias actuales. Habrá que tener en cuenta el manejo de los residuos tecnológicos producto de los nuevos sistemas propuestos.

2.1.5. Agilidad y sencillez

Además de facilitar el recuento de votos se plantea que el voto electrónico puede facilitar el acto mismo de la emisión de cada voto si se implementan soluciones que prioricen la usabilidad y simplifiquen el proceso. Siguiendo esta línea, la interacción de los votantes con sistemas simples y claros también previene errores involuntarios que puedan derivar en votos impugnados (como es el caso de las boletas apócrifas, por ejemplo).

2.1.6. Mayor participación ciudadana

Se espera que la ciudadanía se acerque en mayor medida a participar de las elecciones dando por hecho que el sistema será considerado como un sistema transparente, rápido y fácil de usar. Además, en el caso del voto electrónico con modalidad remota la accesibilidad del sistema es aún mayor al no existir la necesidad de trasladarse hasta los centros de votación y dar la posibilidad de extender los horarios de los comicios.

2.1.7. Modernización

No debe menospreciarse la sensación de status y progreso que implica la adopción de nuevas tecnologías. Existe un sesgo cognitivo que hace pensar que lo tradicional es obsoleto mientras que novedoso es superador. En este sentido el sólo hecho de modernizarse se plantea como una ventaja.

2.2. Problemas intrínsecos

Un sistema informático no puede considerarse infalible. De hecho, suelen estar sujetos a constantes parches y actualizaciones para solucionar problemas detectados. Dada su naturaleza tecnológica cualquier sistema de voto electrónico es

vulnerable a fallos. Pero no sólo los errores de programación o las amenazas externas comprometen la seguridad del proceso de votación que utilice componentes tecnológicos. También hay que considerar aspectos derivados de la naturaleza tecnológica en si misma.

2.2.1. Magnitud de los fallos

A diferencia del voto en papel donde las intervenciones con fines de alterar resultados deben realizarse mesa por mesa, una alteración o falla del software de los dispositivos que se utilizan para votar puede implicar un efecto masivo en los resultados.

2.2.2. Necesidad de controlar el voto emitido

En un sistema de voto electrónico la acción de votar ahora incluye un paso extra: el ciudadano debería no solamente emitir su voto sino también realizar el chequeo de que el mismo fue emitido correctamente. Es de esperar que no todos los participantes realicen este último paso, brindando un posible escenario de manipulación de votos.

2.2.3. Mantenimiento y configuración de los dispositivos

Dados los lapsos transcurridos entre la realización de los comicios se deberá ocupar un tiempo y presupuestos considerables en el mantenimiento de los equipos, las actualizaciones pertinentes y la corrección de errores detectados.

2.2.4. Retrasos ante fallos

En caso de que algunas de las máquinas de votación presenten desperfectos en hardware o software se demorarán los tiempos de votación pues se deberán utilizar de manera compartida las máquinas de votación otras mesas. Ni hablar del caso de fallas en el suministro eléctrico.

2.2.5. Imposibilidad de auditar

Se produce una dependencia de personal especializado para poder realizar controles y escapa al ciudadano común la posibilidad de corroborar el correcto desempeño del proceso electoral.

2.2.6. Pérdida de la privacidad

En caso de que la emisión del voto se realice a través de un dispositivo electrónico es complicado garantizar la privacidad. Si el dispositivo de votación es provisto por las autoridades debería demostrarse que no se guardan registros de los votos emitidos. Por otra parte, si el ciudadano emite su voto con un dispositivo propio el riesgo sería aún mayor por la posibilidad de contener malware que registre o hasta modifique su elección.

2.3. Vectores de ataque

Los siguientes son algunos de los posibles mecanismos a través de los cuales podría vulnerarse el sistema de voto electrónico (el voto en papel también es susceptible a algunos de estos). Cualquier desarrollo debería contemplar la forma de estar protegido frente a estas amenazas.

2.3.1. Máquinas de votación hackeadas

Así como se diseñan técnicas y programas para intervenir o alterar el normal funcionamiento de los sistemas informáticos actuales, los procesos de votación que se apoyen en la tecnología podrían ser víctima de ataques dirigidos a alterar los resultados, conocer la opción seleccionada por los votantes o simplemente atentar contra la disponibilidad del sistema. El software a utilizar, su calidad y la seguridad que sea capaz de brindar es un factor crítico para el éxito de un sistema de voto electrónico.

2.3.2. Ataques a la red

De la misma manera que los dispositivos, la red sobre la cual se apoya el sistema de votación podría ser blanco de intentos de vulnerar la privacidad del voto. Por otro lado, los ataques de denegación de servicio (DoS) son una amenaza siempre latente que pone en jaque la disponibilidad de los sistemas. En un contexto electoral incluso es factible que un ataque DoS se realice de forma selectiva en algunas áreas específicas para alterar los resultados de la elección (por ejemplo, dificultando la votación en lugares donde se estima que algún candidato tiene ventaja sobre otros).

2.3.3. Daños al hardware

Tanto las máquinas de votación como los equipos, los servidores, el cableado y los dispositivos que mantienen activos los canales de comunicación requeridos durante todo el proceso de votación pueden sufrir algún tipo de daño de forma intencional o accidental (hasta incluso por motivos climáticos o ambientales).

2.3.3. Manipulación de resultados

Las autoridades y el personal intervinientes pueden tener interés en el resultado de la votación. No debe ser posible que ellos intervengan agregando, modificando o eliminando votos emitidos.

2.3.5. Voto no autorizado

El sistema puede ser blanco de intentos de emisión de votos por parte de individuos no autorizados. Una de las claves se encuentra en el correcto diseño de la etapa de registro de votantes y el proceso de autenticación de los mismos.

2.3.6. Voto múltiple

Se debe contemplar que todo aquel que se encuentre autorizado para votar solamente pueda hacerlo una vez y evitar así la adición de votos ilegítimos. Un caso especial son aquellos sistemas que permiten a una persona votar múltiples veces, pero sólo contabilizan el último voto emitido.

2.3.7. Coerción

Una de las formas más comunes de influir en las elecciones es condicionar la voluntad de los votantes a través de incentivos o amenazas. Para evitar esto será necesario que el atacante no pueda conocer fehacientemente el voto emitido por su víctima e inclusive que, aún queriendo hacerlo, el votante no pueda demostrar la opción seleccionada. También hay que tener en cuenta la posibilidad de la entrega o sustracción de credenciales para emitir votos en nombre de otros y la coerción a partir del impedimento del voto.

A modo de síntesis se presenta a continuación una comparativa de los vectores de ataque recién mencionados en contraste con las propiedades de seguridad de la información que ponen bajo amenaza:

Vector de ataque al voto electrónico	**Propiedades de seguridad de la información comprometidas**
Máquinas de votación hackeadas	❑ Privacidad ❑ Integridad
Ataques a la red	❑ Disponibilidad ❑ Robustez
Daños al hardware	❑ Disponibilidad ❑ Robustez
Manipulación de resultados	❑ Integridad ❑ Auditabilidad
Voto no autorizado	❑ Integridad
Voto múltiple	❑ Integridad
Coerción	❑ Privacidad ❑ Integridad

Tabla 1 - “Vectores de ataque al voto electrónico vs Propiedades de seguridad de la información comprometidas”. Fuente: elaboración propia.

3. Paradigmas para el diseño de sistemas electrónicos de votación

3.1. Independencia del software

Los llamados sistemas de votación independientes del software son aquellos en los cuales ninguna falla de carácter informático es capaz de provocar un error indetectable en los resultados de la elección, debido a los procesos de verificación y toma de evidencia con los que cuentan (los cuales pueden ayudar a validar que el software funcionó de manera correcta). Un sistema de votación que no sea independiente del software no podrá proporcionar resultados convincentes.
Este concepto fue desarrollado por Rivest y Wack y expresa de forma clara que no se debe depositar la confianza en el correcto funcionamiento del software del sistema de votación. Posteriormente se definió una extensión de este atributo y se dice que un sistema de votación es fuertemente independiente del software si es independiente del software y además un error en la elección (debido al software) puede ser corregido sin la necesidad de volver a realizar la votación.

3.2. Verificabilidad de extremo a extremo

La verificabilidad de extremo a extremo (E2E-V por su sigla en inglés) es uno de los atributos que los sistemas de voto electrónico suelen ofrecer como aval de su independencia del software. De hecho, también trae implícita la independencia del hardware y de los proveedores de sistemas.
Los sistemas E2E-V facilitan maneras de verificar que los resultados de la elección sean correctos detectando errores en las etapas de emisión del voto y recuento. Esto también se realiza de forma electrónica (no se apoyan en recuentos de boletas de papel u otro tipo de soportes físicos).
Para que un sistema cumpla con la verificabilidad de extremo a extremo será necesario que contemple estas cuestiones fundamentales:

1) Que los votantes puedan por sus propios medios verificar que su elección fue registrada correctamente.
2) Que los votantes puedan por sus propios medios verificar que su voto fue contabilizado.
3) Que cualquier persona pueda verificar que todos los votos correctamente emitidos fueron contados.

Aún así, es de destacar que E2E-V se apoya en un supuesto de confiabilidad al menos polémico: la auditoría iniciada por el votante.
Otorgar la capacidad de verificar el correcto funcionamiento del sistema de votación a los propios votantes sólo es útil si ese poder es ejercido. Se necesita que al menos una pequeña fracción del electorado se tome la molestia de realizar el chequeo de la información para proveer la evidencia necesaria de que el resultado presentado es correcto.

Este factor imprevisible también implica que mientras más votos mal registrados o no contabilizados hubiera, entonces menor sería la cantidad necesaria de electores que efectúen la verificación hasta descubrir un fallo. El votante también tiene en sus manos la decisión de chequear la correcta encriptación de su voto, la presencia de su voto encriptado en el conteo de resultados, ambas cosas o ninguna de ellas.
Los sistemas E2E-V implementados en la actualidad plantean una nueva capa de complejidad: las verificaciones que pueden realizar los votantes comprenden la realización de cálculos e interpretaciones que exceden la capacidad humana y por lo tanto deben hacerse con la ayuda de algún software para tales fines. Esto dispara el nuevo interrogante de cómo confiar en dicho software. Una posible solución a este problema es la posibilidad de que cualquiera pueda proveer su propia versión del software de verificación, de modo que se generen alternativas de código abierto y proyectos impulsados por cualquiera de los interesados, generando además multiplicidad de opciones de chequeo para que el votante pueda elegir la que considere apropiada y fortaleciendo la confiabilidad del sistema en general.
Como corolario, cualquier error detectado en un sistema E2E-V implica un mal funcionamiento del software que este ejecuta (ya sea para encriptar los votos o para contabilizarlos) y por lo tanto impugna los resultados que este pueda presentar.
Un buen sistema E2E-V debe detallar cómo proceder en la resolución de conflictos. Esto incluye qué acciones se deben llevar a cabo para reportar un error y cómo las autoridades pueden corroborar que en efecto ese error existe.
La verificabilidad de extremo a extremo proporciona interesantes mejoras en la seguridad de un sistema de votación electrónica, específicamente en lo que se refiere a preservar la integridad de la información y velar por la auditabilidad. Sin embargo, hay que remarcar que otros atributos deseables como la usabilidad y la no coerción están lejos de ser cumplimentados por los sistemas E2E-V analizados.

3.3. Auditorías limitantes del riesgo

Un camino alternativo y a la vez complementario a la verificación individual que puedan llevar a cabo los votantes es aplicar procesos estadísticos para evaluar correctamente pequeñas muestras de los votos emitidos.
Las auditorías limitantes del riesgo son un tipo de auditoría post elección (puesto que se enfoca en revisar los resultados en lugar del procedimiento) y los sistemas de votación que pretendan implementarlas necesitan emitir algún comprobante de votación en papel al momento de emitir cada voto.
El caso más emblemático de aplicación de auditorías limitantes de riesgo son las elecciones con boletas de papel marcadas por los votantes y con contabilización automática mediante sistemas ópticos.

3.4. Privacidad eterna

El concepto de privacidad eterna surge como respuesta al interrogante de qué ocurriría si eventualmente en el futuro el algoritmo utilizado para encriptar fuese

quebrado. Frente a este escenario, si algún interesado pudiera obtener una copia de los votos encriptados sólo tendría que conservarlos con la esperanza de que con el tiempo se encuentre la manera de desencriptarlos en el futuro cuando el poder computacional lo permita o cuando se encuentre alguna vulnerabilidad en el método de cifrado.

Dada su complejidad y la necesidad de conocimientos avanzados en criptografía, en la actualidad no hay sistemas de voto electrónico que implementen privacidad eterna.

4. Primitivas criptográficas

En este capítulo se presentan desarrollos, técnicas y herramientas que sin dudas pueden ser de utilidad en la construcción de sistemas de voto electrónico para proveer seguridad en las diferentes etapas del proceso. La criptografía es clave para proteger la privacidad e integridad de los datos de la elección.

4.1. Esquema de Shamir (Shamir's Secret Sharing)

El esquema de Shamir [27] permite compartir información de manera secreta entre un número n de participantes de forma tal que no sea posible reconstruir dicho secreto sin la colaboración de al menos una cantidad t ($t < n$) de los participantes. Su funcionamiento se basa en la propiedad de que un polinomio de grado m puede ser definido unívocamente por m+1 puntos de la curva.
Esta técnica ayuda a repartir la seguridad entre varios colaboradores a la vez que aumenta la protección frente a pérdidas.
En el contexto de un sistema de voto electrónico este esquema podría utilizarse por ejemplo para compartir claves en que correspondan a las autoridades de la votación. De esta forma para acceder a la clave habría que vulnerar a varios de los participantes.

4.2. Firma grupal (Group signature)

Una firma grupal [16] es un tipo de firma en la cual, constituido el grupo, cualquiera de los miembros del mismo (pero nadie que no sea miembro) puede firmar un mensaje. El receptor del mensaje podrá verificar que la firma corresponde al grupo en cuestión, pero no tendrá manera de descubrir cuál de los miembros realizó la firma. En el caso ideal, un protocolo de firma grupal debería proveer un mecanismo para resolución de disputas, permitiendo revelar la identidad del quien aplicó la firma en caso de ser necesario.
Esta característica busca preservar el anonimato del firmante a la vez que garantiza su aptitud para realizar la firma.

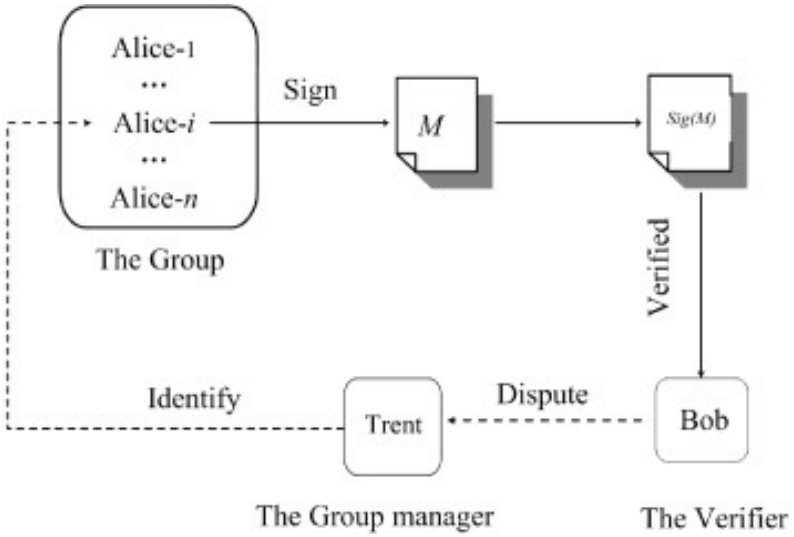

Imagen 2 - Esquema de firma grupal con resolución de disputas. Fuente [31]

Se puede pensar al conjunto de todos los votantes habilitados en una elección como un grupo en el cual todos sus participantes tienen la potestad de firmar un mensaje. Un voto firmado sería válido a los ojos de la autoridad, pues provino de alguno de los votantes habilitados, sin vulnerar la privacidad de su emisor.

4.3. Firma ciega (Blind signature)

La propuesta en este caso es que una autoridad pueda firmar un mensaje, pero sin la posibilidad de acceder a su contenido [10, 11].
El emisor del mensaje lo envía encriptado con su clave privada, pero aplicando previamente una función matemática que lo modifica ligeramente al agregarle un factor aleatorio (también llamado factor de cegado). La autoridad desencripta el mensaje con la clave pública del emisor, pero el contenido es ilegible por el agregado que contiene. Firma el conjunto y lo devuelve al emisor el cual es capaz de remover el factor aleatorio del conjunto firmado obteniendo entonces su mensaje original firmado por la autoridad sin haberlo expuesto.

4.4. Cifrado Homomórfico (Homomorphic encryption)

Esta técnica también puede tener utilidad para el desarrollo de sistemas de voto electrónico, en especial para poder contabilizar los resultados sin vulnerar el secreto del voto.
Un esquema que contenga cifrado homomórfico tiene la propiedad de poder realizar operaciones directamente sobre texto cifrado sin la necesidad de desencriptarlo previamente y tener que volver a encriptar el resultado.
Un ejemplo de criptosistema que cumple esta propiedad es el cifrado de ElGamal [19], donde se tiene:

- Un grupo G con clave pública (G, q, g, h), $h = g^x$ y x como la clave privada
- Un mensaje m que se encripta con $\mathcal{E}(m) = (g^r, m \cdot h^r)$ con un r aleatorio

Como resultado se cumple

$$\mathcal{E}(x_1) \cdot \mathcal{E}(x_2) = (g^{r_1}, x_1 \cdot h^{r_1})(g^{r_2}, x_2 \cdot h^{r_2}) = (g^{r_1+r_2}, (x_1 \cdot x_2)h^{r_1+r_2}) = \mathcal{E}(x_1 \cdot x_2)$$

Resultando que la multiplicación de los mensajes cifrados es equivalente al cifrado de la multiplicación de los mensajes en texto plano.
Como se ha dicho en párrafos anteriores, en el caso del voto electrónico la operación de interés es la suma de los votos encriptados. Si los votos se registran y se almacenan encriptados se quiere obtener enc(a+b) sin tener que desencriptar enc(a) y enc(b). De esta manera el conteo puede realizarse de manera segura y la desencriptación recién se llevaría a cabo sobre el total de los votos sumados.

4.5. Permutación criptográfica (Cryptographic shuffling)

La idea de una permutación criptográfica es transformar una lista de elementos encriptados en una lista alterada mediante permutaciones que pueda ser luego desencriptada sin poder vincular los elementos de la lista inicial con los resultados obtenidos. Las permutaciones deben poder aplicarse siendo lo suficientemente aleatorias pero manteniendo la posibilidad de verificar su correctitud.
En escenarios de votación esta idea puede aplicarse distribuyendo las tareas de permutar elementos y desencriptar entre distintas autoridades. Una vez que los votos fueron permutados, su desencriptación puede publicarse para que el conteo se lleve a cabo de forma pública.

4.6. Cifrado de clave pública (Public key encryption)

La mayoría de los sistemas de voto electrónico utilizan cifrado de clave pública. Su implementación se sustenta en la técnica de doble ensobramiento: en primer lugar, el votante utiliza la clave pública de las autoridades de la elección para cifrar su voto. A este texto cifrado luego le aplicará su propia clave privada para firmarlo.
De esta forma las autoridades en una primera etapa podrán verificar que los votos fueron firmados por votantes habilitados (pues las autoridades cuentan con las claves públicas de los votantes). A los votos válidos se les removerá la firma y serán almacenados de forma que no sean trazables hasta su emisor para proceder al conteo de votos.

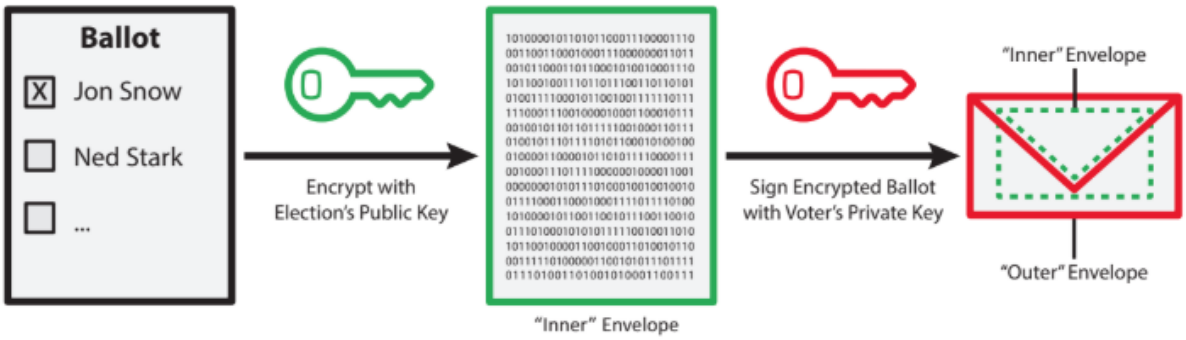

Imagen 3 - Técnica de doble ensobramiento usando criptografía de clave pública. Fuente: [21].

Si alguien intercepta el sobre doble podrá ver quiénes han emitido el voto pero no sabrán cuál fue su elección.
Hay que tener en cuenta que se requiere de una infraestructura (PKI) considerable y la encriptación y desencriptación puede llevar tiempo.

4.7. Pruebas de conocimiento cero (Zero knowledge proofs)

El propósito de las pruebas de conocimiento cero es que una las partes pueda demostrarle a la otra la posesión de un secreto pero sin revelarle el contenido del secreto.
El poseedor del secreto deberá responder una serie de desafíos, los cuales podrá responder sin problemas si efectivamente posee el secreto y en caso de no poseerlo sólo podrá responder correctamente con una probabilidad de ½. La prueba puede repetirse varias veces, disminuyendo con cada iteración las posibilidades de engañar al otro simplemente adivinando la respuesta.
Estas pruebas pueden ser interactivas o no interactivas, dependiendo de si ambas partes deben comunicarse entre sí.
El uso que un sistema de voto electrónico puede darle a las pruebas de conocimiento cero es para proveer verificabilidad a algún paso específico del proceso. Sería importante que las pruebas sean no interactivas para economizar recursos.

4.8. Redes de mezclado (Mix-nets)

Las redes de mezclado o permutación, o simplemente mix-nets utilizan el mismo principio que la red Tor aplica para lograr el anonimato del tráfico de sus usuarios a través de la red: se utilizan muchos mix-servers para cifrar mensajes a través de múltiples capas. El concepto fue originalmente desarrollado para el envío de correo electrónico manteniendo un canal anónimo [12].
Una mix-net se compone de uno o más servidores dispuestos en varias capas. Cada uno de los mix-servers se ocupa de recibir información, encriptarla y permutarla antes de reenviarla a un servidor de la siguiente capa. La corrección de los datos se consigue con pruebas de conocimiento cero entre capa y capa.

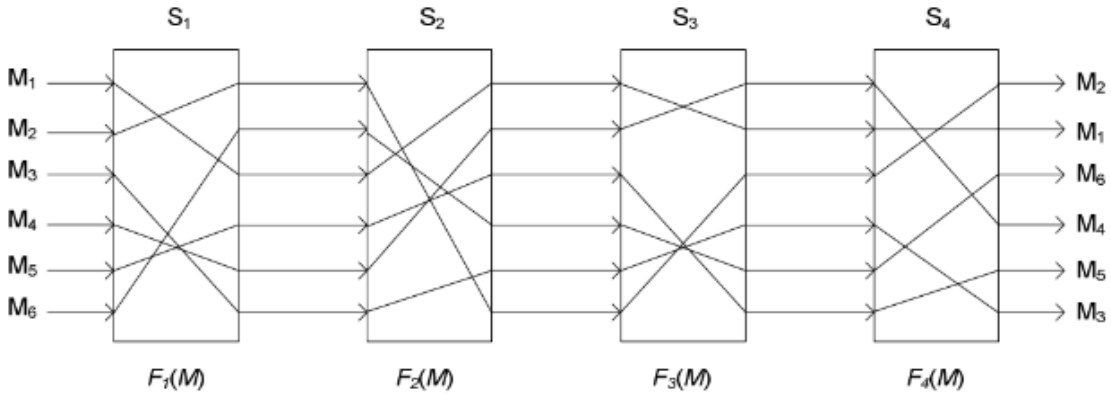

Imagen 4 - Esquema de una mix-net. Fuente: [22]

Una estructura de mix-servers puede implementarse para anonimizar los votos separando el voto encriptado de la firma de su emisor y evitando que esa relación pueda deducirse posteriormente. Funcionan como un complemento adecuado para la técnica de doble ensobramiento.
Nuevamente hay que tener en cuenta la infraestructura, el uso de recursos y los tiempos que agregan las sucesivas encriptaciones. Dicho sea de paso, se requiere un esquema de encriptación que pueda soportar ser encriptado varias veces.

5. Implementaciones destacadas

Esta sección presenta una variedad de sistemas de voto electrónico que gozan de un alto grado de aceptación en la literatura especializada.
El criterio utilizado para evaluar cada uno de estos esquemas es detectar las ventajas y desventajas que presentan para luego determinar en qué grado cumplen con las propiedades de los sistemas de votación seguros vistas en el capítulo 1.

5.1. Voto electrónico presencial (e-voting)

5.1.1. Scantegrity

Scantegrity [14], en su primera versión, fue desarrollado en 2008. Tiene como principio de funcionamiento la combinación de boletas físicas de papel con la tecnología de reconocimiento óptico, la cual en la actualidad se encuentra altamente desarrollada y con un buen grado de adopción entre el público general.
En las boletas utilizadas en este sistema se listan los candidatos asignándole a cada uno un código de letras de forma aleatoria. El votante marcará su elección sobre el papel. Además se agrega un código identificador de la boleta en forma de texto legible y también en forma de código de barras. Este código se presenta en una de las esquinas del papel de forma troquelada para que el votante se lleve ese trozo de la boleta como comprobante de su voto.
Cuando la votación finaliza se escanean las boletas con el objetivo de computar los resultados. Cada voto se almacena en una base de datos anonimizada.
Posteriormente las autoridades publican todos los identificadores de las boletas junto con el código que se eligió en cada una, de forma que los votantes puedan comprobar que sus votos fueron correctamente contabilizados. Dar a conocer el código de letras de la boleta no revela frente a terceros cuál fue el candidato elegido pues los códigos se asignaron a los candidatos de manera aleatoria.

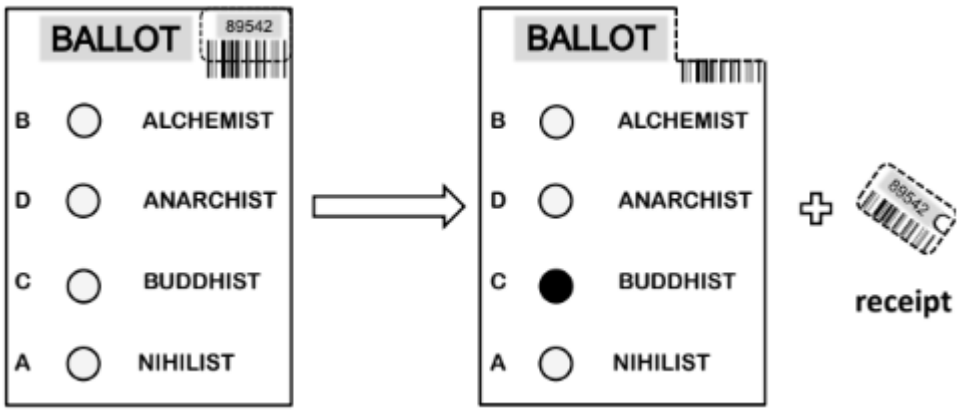

Imagen 5 - Boleta de Scantegrity. Fuente [2].

Para facilitar la resolución de disputas y ayudar a prevenir la coerción, se le hicieron modificaciones al sistema y de esa forma surgió la segunda versión del sistema:

Scantegrity II [13]. Esta nueva versión propone que los códigos aleatorios que tiene cada candidato tengan mayor complejidad y además sean revelados sólo al momento de marcar la boleta (usando una tinta y un marcador especiales). Los votantes, a su vez, se responsabilizan de copiar ese código en el troquel que se llevan para poder verificar el voto posteriormente.

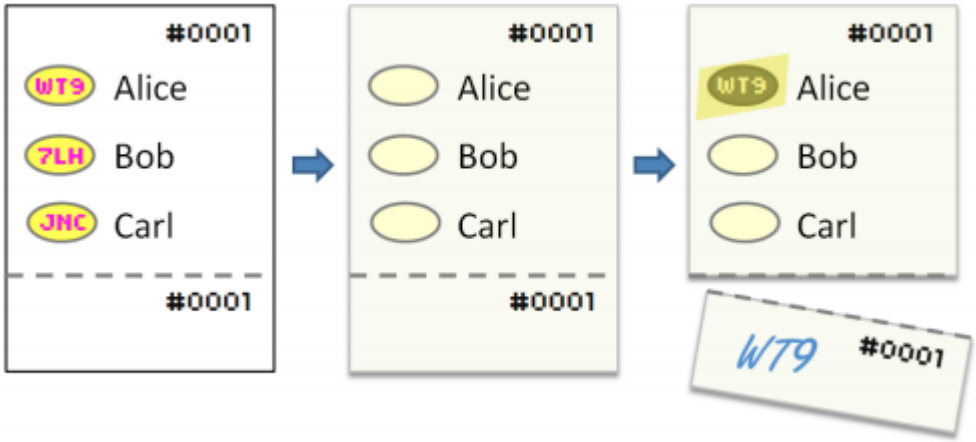

Imagen 6 - Boleta de Scantegrity II. Fuente [13]

Scantegrity II fue utilizado en elecciones municipales en Estados Unidos y a partir de esta experiencia se identificaron mejoras y se recibieron propuestas de los usuarios que derivaron en la tercera versión del sistema: Scantegrity III [15]. Las novedades hacen hincapié en la usabilidad e incluyen la utilización de dispositivos que imprimen los comprobantes de votación firmados digitalmente luego de que el votante haya escaneado la boleta.

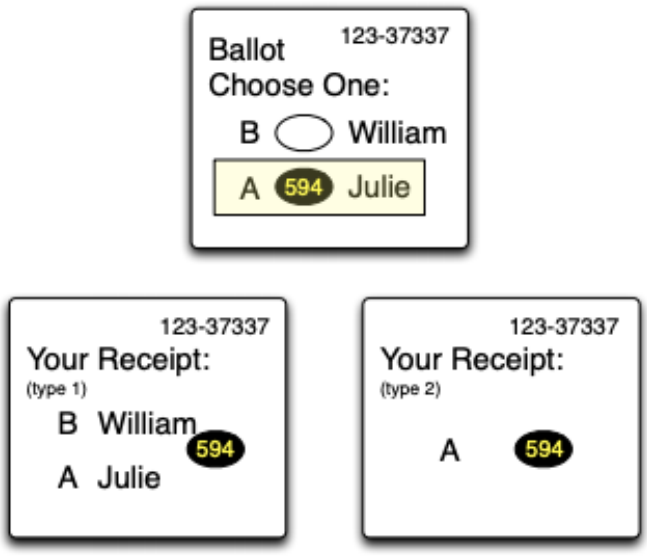

Imagen 7 - Boleta de Scantegrity III con sus dos posibles tipos de comprobante, con cada voto emitido se obtiene un comprobante de uno u otro tipo de forma aleatoria. Fuente: [15].

Ventajas

- Respaldo en boletas de papel físicas.
- Brinda mecanismo de auditoría por parte del votante en el lugar de votación.
- Brinda mecanismo de auditoría por parte del votante finalizada la elección.
- No permite demostrar frente a terceros la opción votada.

Desventajas

- Necesita asumir que las máquinas de votación no serán comprometidas.
- Autoridades maliciosas podrían permitir la emisión de votos ilícitos.
- No depende de las máquinas de impresión de comprobantes pero sí de los dispositivos de escaneo de las boletas.

Propiedad	**Nivel**	**Observaciones**
Privacidad	Medio	Se desacopla la autenticación de la emisión del voto.
Integridad	Muy alto	Se agregaron mecanismos para evitar que las boletas sean modificadas luego de haber sido escaneadas. Los comprobantes de voto son firmados digitalmente.
Disponibilidad	Bajo	El sistema propuesto es centralizado.
Auditabilidad	Alto	Se pueden emitir copias del comprobante de voto sin vulnerar el secreto del voto.
Accesibilidad	Medio	No hay consideraciones especiales para favorecer la accesibilidad.
Usabilidad	Muy alto	El uso del sistema es simple e intuitivo. Fue rediseñado en sucesivas etapas atendiendo el feedback de los usuarios.
Robustez	Medio	En caso de fallas con la impresión de comprobantes se puede continuar manualmente. No hay alternativas ante falla del escáner.
No repudio	Medio	El sistema no define una metodología de autenticación de votantes.

Tabla 2 - Propiedades de seguridad de la información vs su nivel de cumplimiento por parte del sistema Scantegrity. Fuente: elaboración propia.

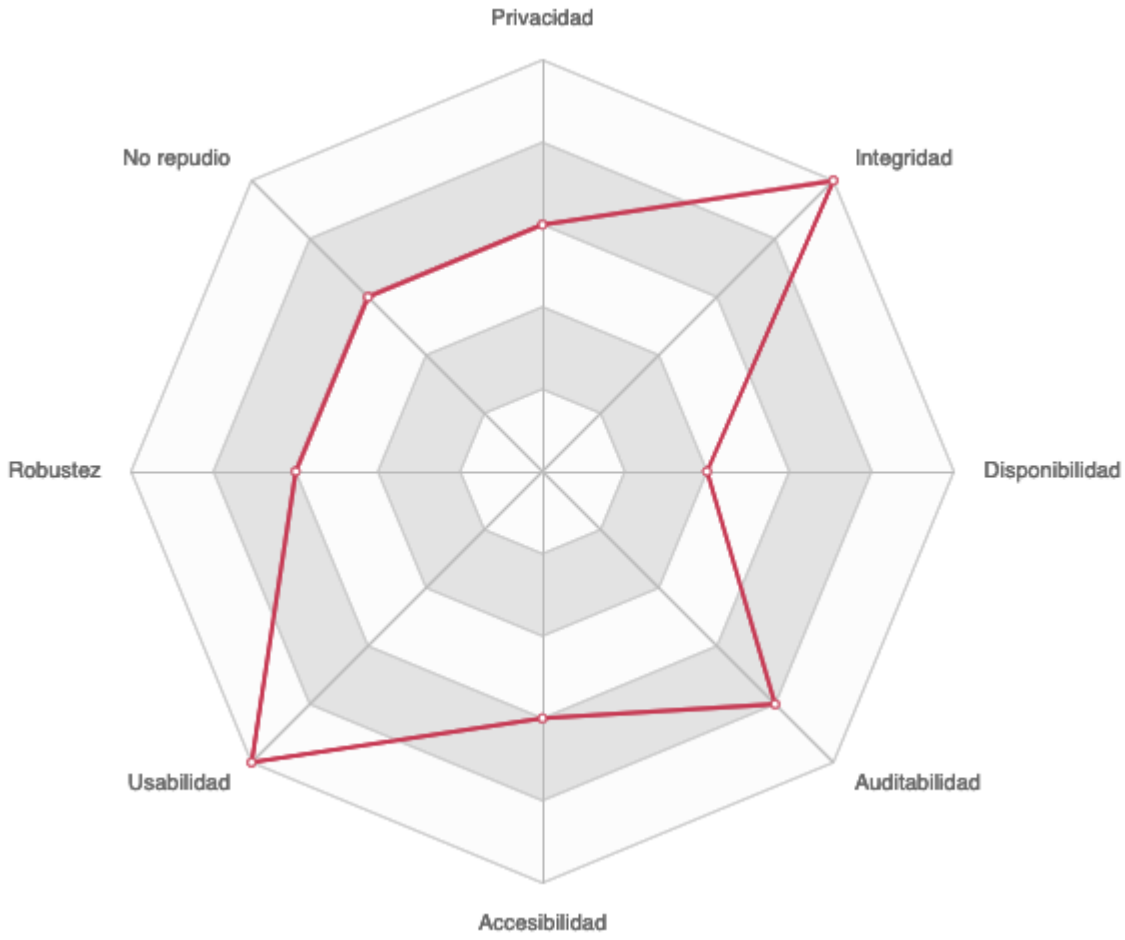

Gráfico 1 - Radar de nivel cumplimiento de propiedades de seguridad de la información por parte de Scantegrity. Fuente: elaboración propia.

5.1.2. Prêt à Voter

Es uno de los sistemas de voto electrónico más destacados y sobre el cual más trabajo se ha dedicado en desarrollarlo y mantenerlo.
Utiliza una boleta de papel con un troquelado que permite dividirla en dos mitades. La mitad izquierda tiene a los candidatos listados en orden aleatorio y en la mitad derecha se encuentran los casilleros para marcar la opción correspondiente junto con una combinación de caracteres alfanuméricos que representa la permutación del orden de los candidatos con respecto a un orden canónico codificada a través de varias capas de encriptación.

Donald	
Barack	X
Alice	
Crystal	
Edward	
	a6Gq21p

Donald	4
Barack	1
Alice	5
Crystal	2
Edward	3
	a6Gq21p

Imagen 8 - Boleta de Prêt à Voter para voto simple (izquierda) y variante para votar por orden de preferencia (derecha). Fuente: [29].

El votante marca su candidato elegido y luego separa las dos mitades. La mitad con los nombres de los candidatos debe destruirla y la mitad derecha escanearla para registrar su voto y conservarla como evidencia. Antes de retirarse puede auditar su voto pidiéndole al sistema que desencripte el código de la boleta para mostrar que el orden al que se corresponde es el mismo que estaba impreso en la mitad izquierda.
Los votos son contabilizados pasando a través de una mix-net que es operada por las autoridades de la elección, quienes utilizan sus claves privadas para desencriptar cada capa.
Al finalizar el proceso eleccionario se publican todas las boletas escaneadas de forma tal que cada votante puede comprobar que su voto haya sido computado. Sin embargo, un votante no puede demostrar ante un tercero que su voto corresponda a algún candidato en particular.

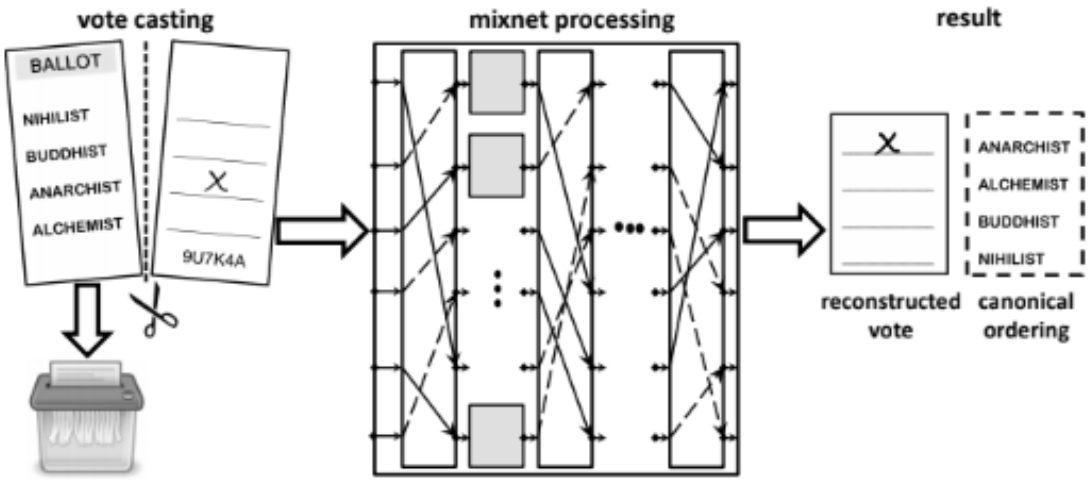

Imagen 9 - Proceso de voto con el sistema Prêt à Voter. Fuente [2].

Ventajas

- Ofrece comprobante del voto que le sirve para auditar.
- Impide demostrar el voto frente a terceros.

Desventajas

- Tiene una fuerte dependencia del sistema de escaneo.

Propiedad	Nivel	Observaciones
Privacidad	Muy alto	Se anonimiza el voto pasando por una mixnet.
Integridad	Medio	Los datos se transmiten encriptados pero no firmados digitalmente.
Disponibilidad	Medio	Su funcionamiento en principio es centralizado.
Auditabilidad	Alto	Los votantes pueden desafiar a la máquina para verificar la correcta encriptación de sus votos.
Accesibilidad	Medio	No hay consideraciones especiales para favorecer la accesibilidad.
Usabilidad	Alto	Privilegia la simplicidad para la emisión de los votos.
Robustez	Bajo	No hay tolerancia ante fallos del sistema.
No repudio	Medio	No se especifica el protocolo para autenticar a los votantes.

Tabla 3 - Propiedades de seguridad de la información vs su nivel de cumplimiento por parte del sistema Prêt à Voter. Fuente: elaboración propia.

Gráfico 2 - Radar de nivel cumplimiento de propiedades de seguridad de la información por parte de Prêt à Voter. Fuente: elaboración propia.

5.1.3. STAR-Vote

La sigla STAR proviene de los términos en inglés Secure, Transparent, Auditable y Reliable. Surgió en el año 2011 por parte de la comunidad académica, a pedido de las autoridades de Texas [28].

STAR-Vote combina el uso de máquinas para emitir los votos (dentro del paradigma de verificabilidad de extremo a extremo) junto con un mecanismo de auditoría en papel.

En el recinto de votación el ciudadano recibe unas credenciales para votar. Estas credenciales le servirán para acercarse hasta una máquina de emisión de votos y hacer su elección. La máquina se encarga de encriptar y grabar el voto emitido. Como resultado se imprime un comprobante con el voto encriptado y algunos datos de referencia (identificación de la máquina, hora de emisión, etc.) para ser depositado en las urnas. También se le da al votante una copia en papel como evidencia de su acción de votar.

Luego de emitir su voto, el ciudadano puede desafiar a la máquina para verificar que la encriptación mostrada sea correcta. Esta acción puede repetirse tantas veces como se crea conveniente hasta y se finaliza con la emisión del voto definitivo.

El conteo se realiza con una suma homomórfica sobre los registros electrónicos de las máquinas. La clave de encriptación es un secreto compartido entre varias autoridades y requiere que todos participen en la recuperación.
Mientras tanto, en paralelo al conteo, se realizan verificaciones y auditorías sobre las boletas de papel que están en las urnas siguiendo el paradigma de auditorías limitantes de riesgo. Un grupo aleatorio de boletas se somete a un doble chequeo: en primer lugar se revisa que los datos en la boleta se correspondan con el registro electrónico y en segundo lugar se comprueba que los resultados obtenidos sobre este subconjunto se aproximen al resultado del conteo electrónico con un margen aceptable.
Finalizada la elección se publican los votos encriptados que fueron contabilizados para que las personas puedan chequearlos con los comprobantes que tienen en su poder.

Ventajas

- Respaldo en papel para auditar la contabilización del voto.
- Posibilidad de desafiar a la máquina para corroborar la encriptación.

Desventajas

- Asume que las máquinas de emisión de votos no serán vulneradas.

Propiedad	**Nivel**	**Observaciones**
Privacidad	Muy alto	La contabilización se realiza sobre votos encriptados utilizando suma homomórfica.
Integridad	Alto	Respaldos en papel de los datos introducidos al sistema.
Disponibilidad	Medio	En principio se trata de un sistema centralizado.
Auditabilidad	Muy alto	Auditorías por parte del votante en el recinto y al publicar los resultados, y también por parte de las autoridades.
Accesibilidad	Medio	No presenta consideraciones especiales de accesibilidad.
Usabilidad	Alto	El circuito de emisión del voto es acotado.
Robustez	Bajo	No hay tolerancia ante fallos del sistema.
No repudio	Alto	El voto se emite con credenciales preparadas para cada votante. A su vez el ciudadano recibe un comprobante del voto.

Tabla 4 - Propiedades de seguridad de la información vs su nivel de cumplimiento por parte del sistema STAR-Vote. Fuente: elaboración propia

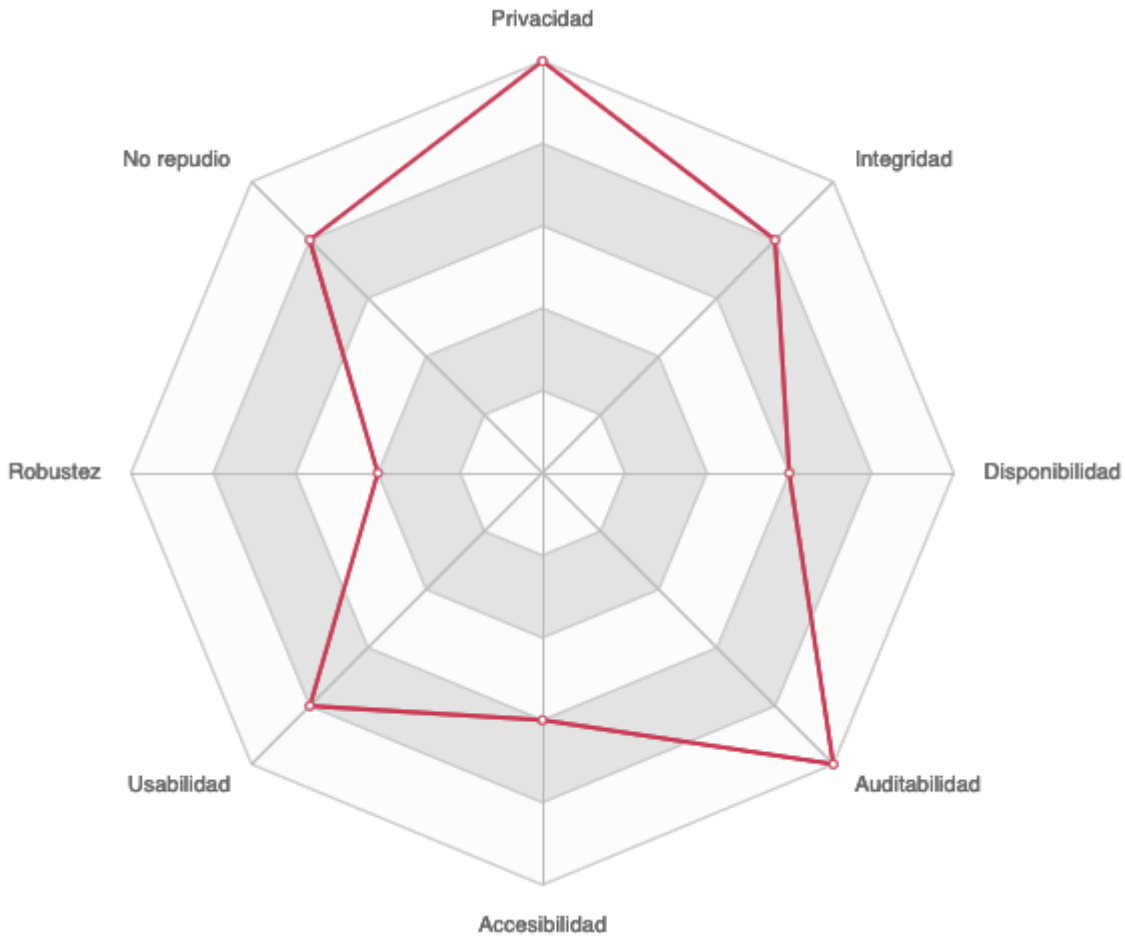

Gráfico 3 - Radar de nivel cumplimiento de propiedades de seguridad de la información por parte de STAR-Vote. Fuente: elaboración propia.

5.2. Voto electrónico remoto (i-voting)

5.2.1. Remotegrity

Fue desarrollado en el año 2013. Remotegrity no es un sistema completo de voto electrónico sino un protocolo de votación online que se combina con sistemas de boletas en papel como Scantegrity o Prêt a Voter cumpliendo el rol de asegurar la correcta entrega de los votos como si hubieran sido emitidos en el lugar de votación de manera presencial.

La persona que desea votar de forma remota recibe por correo previo a la elección una boleta como la de Scantegrity junto con una tarjeta de autorización que contiene un número de serie y tres tipos de códigos: códigos de autorización (varios), un código de bloqueo y un código de confirmación.

El día de la elección el votante entra al sistema online e ingresa el número de serie de su boleta y el número de serie de su tarjeta de autorización (de esta forma el

sistema puede validar que esta persona aún no haya emitido su voto). Luego obtiene de la boleta el código correspondiente al candidato que quiere elegir y lo envía junto con alguno de los códigos de autorización presentes en la tarjeta. Este mensaje se publica en un boletín online. Las autoridades validan el código de autorización, le agregan un código de confirmación y firman el mensaje completo. El registro se actualiza en el boletín. Posteriormente el votante revisa el código de confirmación y valida que su voto no ha sido alterado ingresando el código de bloqueo. Al finalizar la elección las autoridades chequean los códigos de bloqueo y traspasan los votos (código de candidato y número de serie de la boleta) al sistema de conteo presencial. El uso de esta serie de códigos cruzados imparte mayor seguridad contra la alteración del voto, ya sea por parte de terceros o por parte de las autoridades mismas. No obstante, este protocolo no protege de la coerción o la compra de votos.

Ventajas

- Previene el voto múltiple.

Desventajas

- Depende del sistema de distribución de las boletas
- Susceptible a la coerción.

Propiedad	**Nivel**	**Observaciones**
Privacidad	Bajo	No presenta medidas para proteger los canales de comunicación.
Integridad	Muy alto	Sucesivas confirmaciones a ambos lados de la comunicación para preservar la correctitud de la información.
Disponibilidad	Medio	Depende del acceso a internet de los votantes.
Auditabilidad	Medio	Depende del sistema de votación que complemente.
Accesibilidad	Alto	Su carácter remoto favorece la accesibilidad.
Usabilidad	Bajo	El protocolo requiere la ejecución de muchos pasos por parte del votante.
Robustez	Bajo	No presenta consideraciones adicionales para tolerar fallos.
No repudio	Alto	Intercambio de códigos de confirmación.

Tabla 5 - Propiedades de seguridad de la información vs su nivel de cumplimiento por parte del sistema Remotegrity. Fuente: elaboración propia

Gráfico 4 - Radar de nivel cumplimiento de propiedades de seguridad de la información por parte de Remotegrity. Fuente: elaboración propia.

5.2.2. Helios

Es una implementación libre y de código abierto que también puede ser usada de forma online en su sitio web [20]. Actualmente se encuentra en su versión 3, luego de haber incluido mejoras en la privacidad con cifrado homomórfico.

Helios permite que los votantes puedan verificar que sus votos sean agregados al conteo y también que terceros puedan verificar que todos los votos hayan sido contabilizados.

Hay que destacar que no brinda protección contra la coerción pero cuenta con un protocolo para que el votante notifique que está siendo inducido a votar de una forma determinada.

El procedimiento para votar es el siguiente:

1) El sistema de preparación de boletas (Ballot Preparation System - BPS) guía al votante para hacer la selección y guarda su opción seleccionada.
2) La respuesta es encriptada junto con algunos datos aleatorios de respaldo.
3) El votante puede elegir entre auditar el voto encriptado para verificar que efectivamente guarda la respuesta que él eligió o aceptar el voto y enviarlo.

    a) Si el votante elige auditar entonces el BPS le provee el texto cifrado junto con la clave de desencriptación para que se realice la corroboración de que lo que se desencripta coincide con su selección y con los datos aleatorios que se habían agregado como respaldo. El voto vuelve a ser encriptado junto con nuevos datos aleatorios y se le vuelve a dar la opción al votante de auditar o enviar el resultado.
    b) Si el votante elige confirmar, el sistema conserva el voto encriptado y descarta todo el resto de los datos. Se continúa con el siguiente paso.
4) El votante debe autenticarse. Si lo hace correctamente su voto es entonces registrado.
5) Helios provee el llamado botón de notificación de coerción, el cual en caso de activarse envía el texto cifrado, los datos aleatorios y el texto plano a una dirección de correo electrónico ingresada por el votante.
6) Se publican todos los votos encriptados a medida que se emiten, de modo que todo aquel que haya votado pueda verificar que su voto esté presente en el conteo.
7) Finalizada la elección las autoridades computan los resultados sumarizando los votos encriptados. En este paso se utiliza cifrado homomórfico.
8) Se publican los resultados de la elección. Todos pueden verificar que sus votos están presentes y que el conteo fue correcto.

Es verdad que Helios cumple con las consignas de E2E-V y permite que los votos sean verificados, sin embargo hay algunas cuestiones quedan sin resolver. Más allá de su vulnerabilidad a la coerción (la cual según sus desarrolladores es un problema inherente al voto electrónico remoto) también se necesitan formas de probar que no se agregaron votos fraudulentos al conteo usando las identidades de votantes que no hubieran emitido su voto durante el tiempo destinado a la elección.

Ventajas
- Implementación con código open source.
- Permite verificar el voto encriptado antes de enviarlo.

Desventajas
- Susceptible a la coerción
- Podría contabilizar votos fraudulentos.

Propiedad	**Nivel**	**Observaciones**
Privacidad	Medio	El voto viaja con cierto grado de encriptación y en la contabilización se utiliza una suma homomórfica.
Integridad	Medio	No se utiliza firma digital para garantizar la integridad de la información.

Disponibilidad	Medio	Depende del acceso a internet de los votantes.
Auditabilidad	Muy alto	Los votantes pueden desafiar al sistema para verificar la correcta encriptación de sus votos. Se publican los votos encriptados para que la contabilización pueda ser auditada.
Accesibilidad	Alto	Su carácter remoto favorece la accesibilidad.
Usabilidad	Alto	El circuito de emisión de votos es acotado.
Robustez	Bajo	No presenta consideraciones adicionales para tolerar fallos.
No repudio	Bajo	Presenta problemas de suplantación de identidad.

Tabla 6 - Propiedades de seguridad de la información vs su nivel de cumplimiento por parte del sistema Helios. Fuente: elaboración propia.

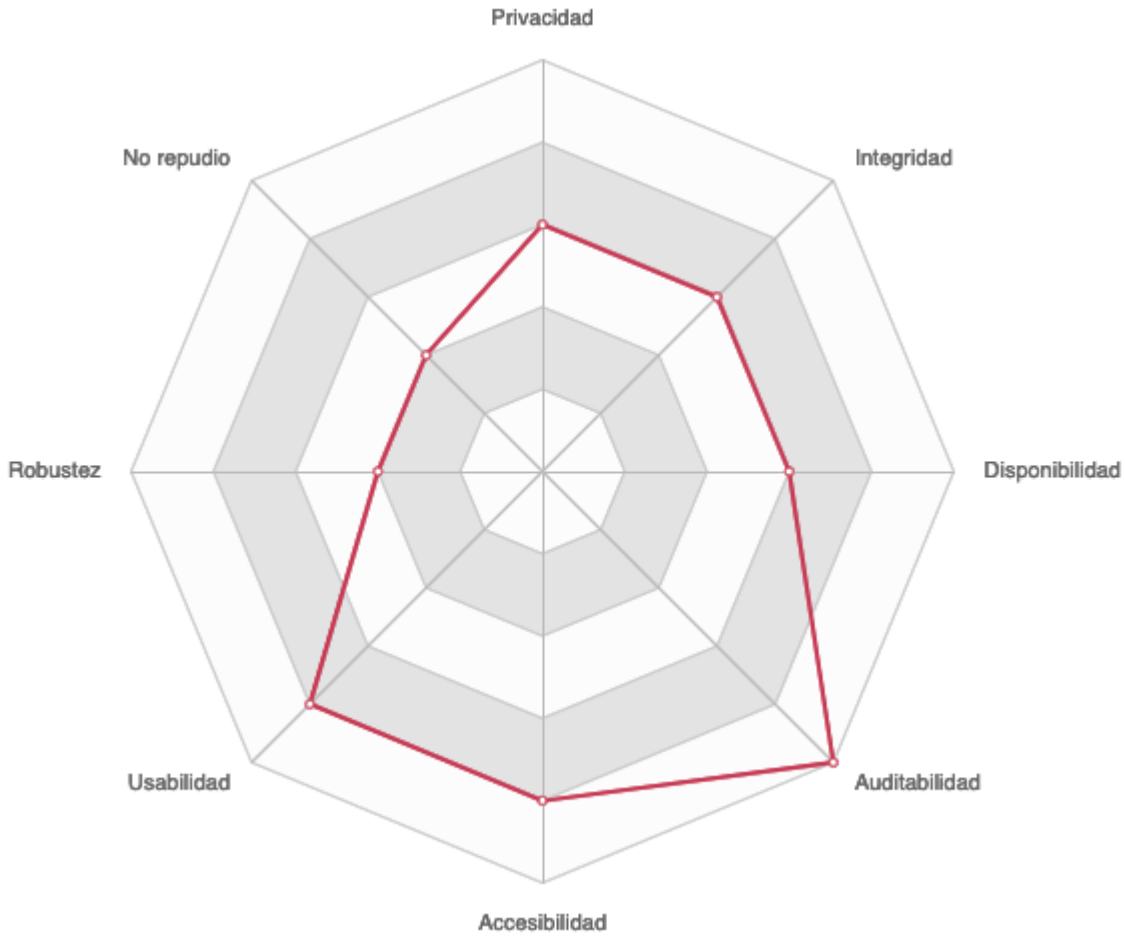

Gráfico 5 - Radar de nivel cumplimiento de propiedades de seguridad de la información por parte de Helios. Fuente: elaboración propia.

5.2.3. Civitas

Civitas es una propuesta open source de voto electrónico desarrollada por la Universidad de Cornell (Ithaca, New York) [17]. El sistema fue hecho usando el lenguaje de programación Jif (una extensión de Java). No se ha utilizado de manera oficial en elecciones pero sirve como ejemplo de un sistema de votación distribuido, verificable y con algún grado de seguridad. Entre sus características destacadas se encuentra el estar exento de coerción.

En este esquema participan cinco roles (agentes):

- Supervisor - Quien administra la elección
- Encargado del padrón - Quien autoriza el padrón
- Encargados del registro - Quienes generan credenciales para la emisión de votos
- Contador - Quienes contabilizan los votos
- Votantes - Quienes emiten los votos

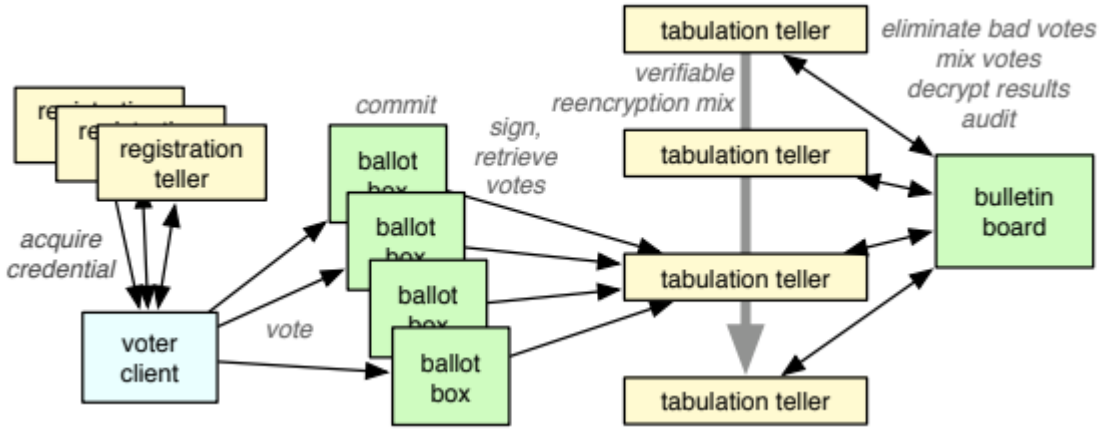

Imagen 10 - Arquitectura del sistema Civitas. Fuente: [17].

Etapa inicial

Como primer paso, el supervisor crea la elección, publicando un boletín con el diseño de la boleta acorde a los parámetros deseados y selecciona a los escrutadores a partir de sus claves públicas.

Luego el encargado del padrón se ocupa de definir los votantes habilitados, creando para cada uno dos claves: una clave de registro y una clave de designación. Se trata de claves basadas en el algoritmo RSA, aunque cualquier otro algoritmo de generación de claves asimétricas puede ser utilizado. Los votantes reciben estas claves antes de la elección.

En tercer lugar los contadores, de manera conjunta, generan una clave pública y la agregan al boletín. Hay que notar que en este paso se emplea el esquema de secreto compartido, de forma que la desencriptación de los mensajes encriptados con esta clave pública necesitará de la participación de todos los contadores.

Por último los encargados del registro generan credenciales, las cuales son pares de claves públicas y privadas para autenticar votos de manera anónima. Cada credencial se encuentra asociada a un votante; las partes públicas de las mismas se agregan también al boletín y las partes privadas se guardan de forma compartida entre los encargados del registro.

Etapa de votación

El votante debe autenticarse frente a un encargado del registro utilizando su clave de registro (la cual recibió con anterioridad, luego de ser generada por el encargado del padrón). Luego de realizada la autenticación, se lleva a cabo un protocolo que utiliza la clave de designación del votante para obtener el fragmento de la parte privada de la credencial del votante que está en poder del encargado del registro. Este procedimiento debe repetirse con todos los encargados del registro de forma tal que, teniendo todos los fragmentos del secreto compartido ellos, pueda reconstruirse la parte privada de la credencial del votante en cuestión.

Con la parte privada de su credencial en su poder, el votante puede emitir su voto en el momento en que lo desee (dentro del plazo establecido para la elección). Para hacerlo deberá enviar su credencial privada y la opción de candidato elegida (ambas encriptadas).

El votante también tiene la posibilidad de generar por sí mismo credenciales falsas, a fin de protegerse de la coerción. También puede emitir su voto más de una vez, en cuyo caso la forma en que se contabilizará su voto dependerá de la política definida por el supervisor dentro de los parámetros de la elección (si se toma por válido el último voto emitido, si se anulan votos duplicados, etc.).

Etapa de conteo de votos

El conteo se realiza de manera colectiva entre los contadores, los cuales recuperan de las urnas los votos emitidos y las credenciales públicas del boletín. Se verifica la correctitud de los votos y se eliminan los que no sean válidos o estén duplicados.

Posteriormente se procede a anonimizar los votos utilizando una mix-net y se eliminan los votos que pudieran tener credenciales falsas. Como último paso se desencriptan los votos (las opciones, no las credenciales) y se publican. Con esta información los resultados son públicamente computables.

Ventajas

- Código open source.
- Separación de roles para tareas específicas.
- Adaptable a múltiples algoritmos de encriptación.
- Contempla una forma de resistir la coerción.

Desventajas

- Depende del sistema de distribución de las claves de los votantes.
- Se asume que el canal de transmisión mantiene el anonimato.
- Bajo nivel de usabilidad.

Propiedad	Nivel	Observaciones
Privacidad	Alto	Se utiliza un complejo sistema de credenciales con claves públicas y privadas. Los votos se anonimizan.
Integridad	Muy alto	Estructura de clave pública con votos firmados.
Disponibilidad	Alto	Está pensado para ser implementado de forma distribuida.
Auditabilidad	Bajo	El votante no puede desafiar al sistema para saber si el código encriptado respeta su opción elegida.
Accesibilidad	Medio	No tiene consideraciones especiales de accesibilidad.
Usabilidad	Bajo	El circuito de emisión de votos es complejo.
Robustez	Bajo	No hay tolerancia a fallos.
No repudio	Medio	Si bien cuenta con un complejo sistema de autenticación para emitir los votos no se entrega un recibo del voto.

Tabla 7 - Propiedades de seguridad de la información vs su nivel de cumplimiento por parte del sistema Civitas. Fuente: elaboración propia.

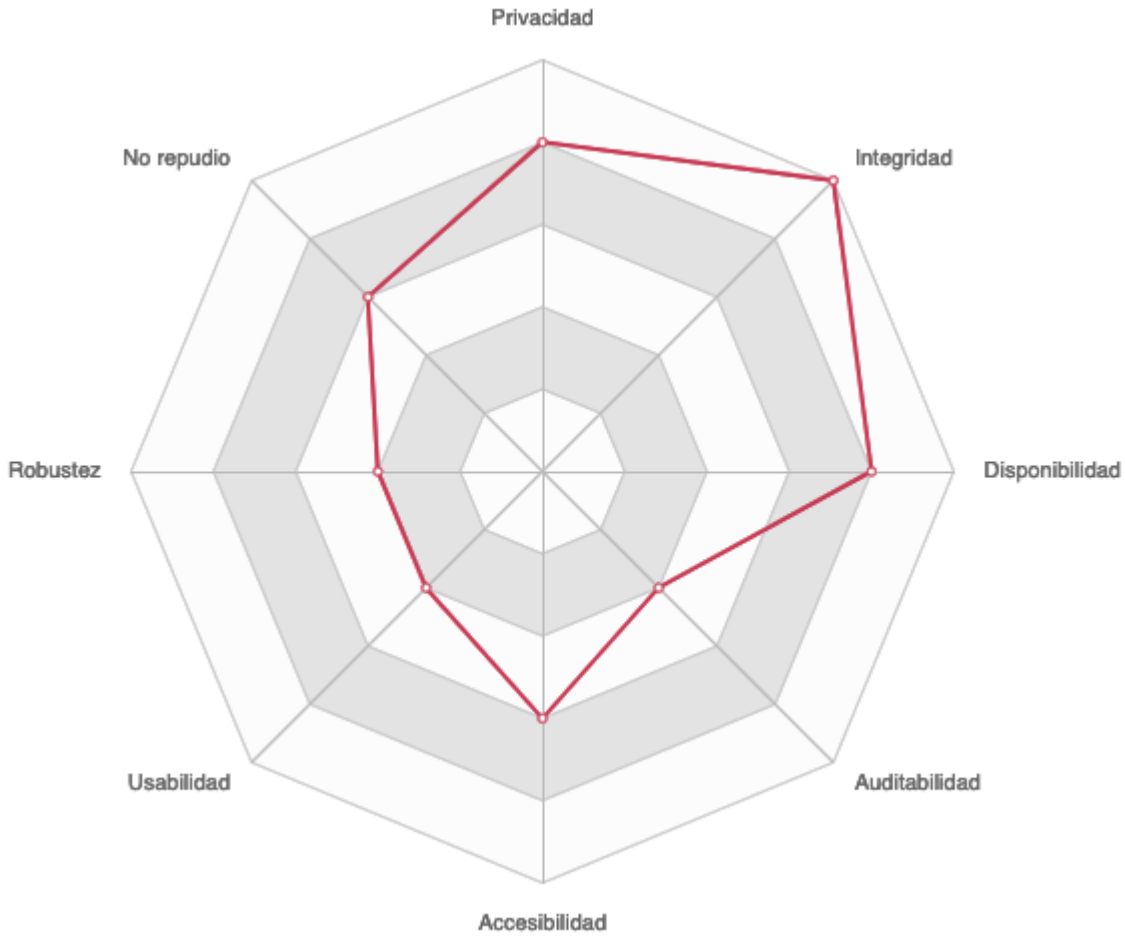

Gráfico 6 - Radar de nivel cumplimiento de propiedades de seguridad de la información por parte de Civitas. Fuente: elaboración propia.

6. Líneas de investigación actuales

En el apartado anterior se mencionaron esquemas de voto electrónico que fueron objeto de varias instancias de análisis y experimentación. Sin embargo, los vertiginosos cambios de escenario que se provocan con cada nuevo avance tecnológico abren las puertas a interesantes variaciones y mejoras para los métodos conocidos.

6.1. Blockchain

En la última década, la aparición de las criptomonedas favoreció la percepción del público general sobre la confiabilidad de los sistemas informáticos. El furor que causó la adopción de Bitcoin y demás monedas virtuales hizo natural que se contemple la implementación de la tecnología en otros ámbitos de la vida: desde contratos inteligentes hasta resolución de disputas usando registros de logs digitales. Los sistemas de votación no quedaron exentos de este movimiento, de manera que han surgido y continúan apareciendo sistemas de voto electrónico que basan su funcionamiento (o al menos una parte de él) en la tecnología de blockchain.

6.1.1. Conceptos básicos de blockchain

Blockchain se presenta como una base de datos distribuida, la cual está formada por una serie de bloques que se referencian entre sí. La información contenida en cada bloque corresponde a transacciones realizadas (la cantidad de transacciones que contiene cada bloque es variable) y para poder agregar un bloque nuevo a la cadena este primero debe ser validado por varios de los nodos que componen esta estructura. El proceso de adición de bloques incluye la llamada prueba de trabajo, la cual consiste en un desafío computacional abierto y transparente que premia al nodo que lo resuelva y puede ser verificado por los demás.
Por la forma de entrelazar los bloques se previene que el contenido de la blockchain pueda ser modificado (editar un bloque implicaría tener que modificar todos los bloques anteriores), logrando así un sistema con información que resulta irrefutable y goza del consenso entre sus partes sin la necesidad de contar con una autoridad centralizada.

6.1.2. Aplicación en sistemas de voto electrónico

Dado que el soporte de estos sistemas es una base de datos distribuida y descentralizada sus puntos fuertes son la integridad de la información (está replicada en cada uno de los nodos de la blockchain), el no repudio de las acciones realizadas y la auditoría abierta. Las transacciones son públicas e inmutables, algo que en principio contribuye a la transparencia del sistema.
Por su carácter tan reciente aún no es posible hablar de implementaciones consagradas o esquemas clásicos que sirvan como modelos de referencia dentro de este apartado. Además la mayoría de las soluciones son ofrecidas por empresas

privadas como plataformas listas para su uso pero sin ser de código abierto [1, 6, 30]. La propuesta entonces es analizar de qué maneras la tecnología blockchain interviene en el diseño de sistemas de voto electrónico dentro de las alternativas conocidas hasta el momento.

El primer aspecto que se puede apreciar es que la blockchain en sí misma cumple la función de tablero de publicación de resultados. La información volcada en esta base de datos se mantiene de manera replicada entre los nodos y accesible para el público general. Con los datos persistidos en la blockchain cada participante podrá realizar la verificación de su voto y la auditoría de resultados correspondiente. De forma general, para agregar datos a la base de blockchain cada voto emitido se impacta como una transacción y todos los interesados estarán de acuerdo en que los votos no fueron modificados o borrados y que no se agregaron votos inválidos (el sistema verifica la transacción antes de agregar el nuevo bloque a la blockchain).

Otro punto a favor de la descentralización es que se evita tener un único lugar de falla o de hackeo y en cambio se tiene una redundancia que incrementa tanto la robustez como la disponibilidad del sistema.

La transparencia del sistema también resulta favorecida puesto que las transacciones se persisten y los resultados se actualizan en cuestión de minutos y a la vista de todos. Habrá que tomar precauciones para que los datos que se van publicando no influyan en las decisiones de los votantes que aún deben emitir su voto.

6.2. Computación cuántica

Hasta ahora, todos los sistemas de voto electrónico que se han presentado en este trabajo basan su seguridad en el supuesto de que hay ciertos problemas cuya resolución es muy complicada a nivel computacional. Las primitivas criptográficas vistas resultan herramientas de suma utilidad si cuestiones como el problema de la factorización de enteros muy grandes presenta un desafío inviable para quien trate de criptoanalizar el sistema. El escenario cambiaría por completo con la aparición de las computadoras cuánticas, las cuales tienen el poder de convertir los asuntos computacionalmente complejos en problemas fácilmente resolubles.

La computadora cuántica es un elemento que a la fecha aún no existe más que en definiciones teóricas, sin embargo se estima que en el corto plazo se hará realidad y hasta se especula con que algunos organismos dedicados al ciberespionaje, tales como la NSA, ya han logrado desarrollar sus propios dispositivos con estas características.

Frente a este panorama los investigadores llevan años analizando la posibilidad de utilizar esta tecnología para construir protocolos de votación electrónica más seguros, aunque también se abre un abanico de ataques nuevos frente a los cuales será necesario levantar defensas.

6.2.1. Conceptos básicos de computación cuántica

Se usa el término de qubit para denominar a la menor partícula capaz de almacenar información cuántica. A diferencia de un bit clásico, el cual puede tomar el valor 0 o 1, un qubit que se encuentre en estado puro puede expresarse como combinación lineal de dos vectores:

$$|x\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \text{donde} \quad |0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

$$|\alpha|^2 + |\beta|^2 = 1$$

donde $|\alpha|^2$ es la probabilidad de que el qubit valga 0 al medirlo y $|\beta|^2$ es la probabilidad de que el qubit valga 1 al medirlo.
Una diferencia importante entre la información cuántica y la información clásica es que no hay mecanismos para copiar estados cuánticos desconocidos. Esta propiedad, llamada teorema de no clonación, tiene grandes implicancias para la computación cuántica.

6.2.2. Protocolos cuánticos para voto electrónico

Los protocolos de computación cuántica aplicables a los esquemas de voto electrónico pueden agruparse en cuatro familias, cada cual con sus propias ventajas y vulnerabilidades, las cuales serán brevemente analizadas a continuación:

- Protocolos de medición de doble base
  El sustento de la seguridad de estos protocolos es la técnica de medición de doble base. Se usan estados entrelazados con la propiedad de que al medirlos en la base computacional, la suma de las salidas es igual a cero y al medirlos en la base de Fourier, todas las salidas son iguales. Su desventaja es la posibilidad de atacar la privacidad de un votante en caso de haber otros votantes maliciosos.
- Protocolos basados en urnas de elección viajeras
  Este tipo de protocolos son de utilidad para referéndums o elecciones de carácter binario. Se prepara un estado entrelazado y se envía para que vaya pasando de votante en votante. Cada uno de ellos realiza una operación unitaria sobre el sistema en base a su preferencia y luego lo pasa al siguiente elector. Cuando todos hubieron votado se mide el estado final del sistema para determinar el resultado. La principal vulnerabilidad que presenta este protocolo es la posibilidad de emitir votos múltiples, al aplicar varias veces la operación correspondiente.
- Protocolos basados en boletas distribuidas
  La manera de efectuar la votación siguiendo este protocolo es repartir una boleta en blanco a cada votante y reunirlas todas después que todos hayan votado para computar el resultado final. Además de ser permeable al voto

múltiple, como en el caso anterior, hay que considerar que se fortalece la privacidad frente a otros votantes pero no ante la autoridad.

- Protocolos basados en codificación conjugada
  La idea principal de estos protocolos es utilizar el esquema de distribución de claves BB84 para agregar mecanismos de verificación del voto. El problema que presentan suele ser el garantizar la integridad de la opción seleccionada por el votante.

Hasta aquí se ha realizado un breve acercamiento a la temática de la computación cuántica y sus implicancias en el posible desarrollo de sistemas de voto electrónico. Lo interesante, más allá de la falta de soluciones concretas, es la cantidad de puertas que se abren para investigaciones futuras.

7. Propuestas para trabajo a futuro

Este trabajo se ha nutrido del fruto de años de investigaciones realizadas a lo largo de todo el mundo y del aporte de una gran cantidad de profesionales que se han interesado por estudiar las particularidades del voto electrónico y han compartido sus hallazgos. El reconocimiento al esfuerzo de la comunidad académica también invita a tener grandes expectativas en los avances que podrán lograrse en un futuro no muy lejano. Por tal motivo se expresan a continuación una serie de propuestas planteadas como disparadores de ideas para continuar con el trabajo de investigación y el desarrollo de nuevas soluciones.

Del análisis realizado en capítulos anteriores se advierte que hay requerimientos de seguridad que son más difíciles de cumplir y por lo tanto los esquemas e implementaciones actuales no los han resuelto o los han cubierto sólo de manera parcial.

En este sentido la incoercibilidad es uno de los grandes desafíos que requiere más estudio y análisis pues a la fecha las medidas para mitigarla implican el seguimiento de protocolos criptográficos difíciles de llevar a la práctica por los votantes o se conforman sólo con su detección pero no la evitan.

Otro de los tópicos que será importante profundizar es complementar la usabilidad y la experiencia de usuario con una efectiva comprensión de los sistemas de voto electrónico a utilizar. Suele confundirse la noción de “saber cómo funciona un sistema” con “saber cómo usar un sistema”. Interactuar de manera intuitiva y agradable puede favorecer la adopción de una solución tecnológica pero el verdadero valor para los votantes se ofrecerá si las personas pueden entender qué es lo que ocurre con la información. Desarrollar sistemas seguros y a la vez comprensibles por el electorado general es una tarea que demandará tiempo y esfuerzo.

A nivel académico teórico quizás los caminos más interesantes para elaborar estudios sean, por un lado, la estandarización de los requerimientos funcionales y no funcionales que debe cumplir un sistema de voto electrónico y por otro el desarrollo de herramientas que sirvan para la evaluación objetiva de los protocolos que siguen apareciendo. Ambos tópicos fueron ligeramente delineados en el presente trabajo con la esperanza de que sean de utilidad para futuros análisis.

Indudablemente todo lo referido al impacto de la computación cuántica en los sistemas informáticos es un terreno fértil para avanzar con las investigaciones (no sólo en cuanto al voto electrónico) y sin dudas atraerá el interés de muchos profesionales de las ciencias de la computación.

8. Conclusiones

¿Qué espera la gente del voto electrónico? Sin dudas existe un factor psicológico que predispone a las personas a buscar el confort y una mejor calidad de vida a partir del uso de la tecnología, o al menos la sensación de bienestar que otorga la modernización aunque su efecto se diluya con el tiempo y en la avidez de seguir avanzando hacia nuevos objetivos.

La sociedad espera con ansias la aparición de una solución que logre transformar las elecciones en un trámite fácil y confiable. Mientras que la facilidad puede percibirse de forma clara a través de resultados instantáneos o interfaces amigables, la confiabilidad de un sistema debe someterse a una evaluación consciente y escéptica por parte de los individuos. Este ejercicio de desconfianza va en contra del sesgo de confirmación que tenemos los seres humanos, el cual nos dificulta encontrar desventajas en aquellas cosas que a priori son beneficiosas. Por el mismo motivo que entregamos información personal a terceros para poder formar parte de las redes sociales o aplicaciones que estén de moda también somos reticentes a admitir los riesgos a los que nos exponemos sólo para no resignar los beneficios que se obtienen.

También es verdad que la apatía de los más jóvenes hacia la participación en la vida ciudadana puede combatirse ofreciéndoles herramientas atractivas y más cercanas a sus intereses y el voto electrónico es una alternativa seductora para las nuevas generaciones que crecieron utilizando dispositivos y sistemas informáticos con naturalidad como parte de su vida.

Lo cierto es que, dada la importancia de lo que está en juego en una elección, cualquier solución debería implementarse de manera gradual y sin apuros. No hay que perder de vista que debe priorizarse la eficacia por sobre la eficiencia (es mejor hacerlo bien que hacerlo rápido). Para aventurarse a hacer el cambio a un nuevo sistema se debería comprobar primero que la alternativa propuesta es mejor que el sistema actual, es decir que no alcanza con intercambiar unas falencias por otras ni conformarse con que el voto electrónico “no es peor” que el voto en papel.

En los diversos capítulos de este trabajo se ha tratado de presentar diferentes aspectos de la tecnología aplicada a los sistemas de votación. Se han analizado interesantes beneficios potenciales a la vez que preocupantes riesgos de seguridad aparecen en escena. Es indudable que la labor de especialistas académicos y teóricos puede contribuir a desarrollar herramientas para fortalecer cualquier proceso electoral, pero cada propuesta estará completa y será realmente útil si se aceptan sus aspectos positivos sin disimular los negativos.

Las diferentes formas de implementar el voto electrónico y los esquemas en los cuales se basan comparten la particularidad de dejar cabos sueltos sin atender. Los trabajos que proponen sistemas de votación infalibles se apoyan en supuestos y limitaciones al alcance que plantean la duda sobre la posibilidad de su puesta en práctica.

Sustituir riesgos actuales por nuevos riesgos no parece ser el camino más beneficioso. La ausencia de incidentes no es un comprobante de mitigación de riesgos, las medidas preventivas deben aplicarse dando por sentado que esos riesgos efectivamente pueden ocurrir.

Por otra parte se ha visto que el concepto de computación cuántica, sus protocolos, ataques y técnicas de defensa aún sin haberse materializado ya representan una amenaza a los esquemas de voto electrónico basados en criptografía moderna cuya implementación se continúa debatiendo.

Finalmente remarcar que se espera que este trabajo contribuya para dejar más claro el panorama actual en el estudio del voto electrónico y que pueda ser tomado como punto de partida para continuar investigando, experimentando y buscando alternativas para mejorar la vida de las personas sin perder de vista el valor de la seguridad de la información.

Un tema tan amplio, sensible y controversial como el que ocupa estas páginas aún será motivo de mucha investigación y trabajos. Y está bien que así sea.

9. Bibliografía

[1] Agora Whitepaper, https://www.agora.vote/s/Agora_Whitepaper.pdf (consultado el 02/07/2019)

[2] Ali, S. T. y Murray, J., “An Overview of End-to-End Verifiable Voting Systems”, *Real-World Electronic Voting: Design, Analysis and Deployment*. CRC Press, pp. 171-218, 2016.

[3] Arapinis, M., Kashefi, E., Lamprou, N., Pappa, A., “A Comprehensive Analysis of Quantum E-voting Protocols”. In: arXiv preprint arXiv:1810.05083, 2018.

[4] Benaloh, J., Rivest, R., Ryan, P. Y. A., Stark, P., Teague, V., & Vora, P. End-to-end verifiablity, 2013.

[5] Bernhard, M., Benaloh, J., Halderman, J., Rivest, R., Ryan, P., Stark, P., Teague, V., Vora, P., Wallach, D. S., Public evidence from secret ballots. In E-Vote-ID’17: 10th International Conference for Electronic Voting, LNCS, pp. 84–109. Springer, 2017.

[6] Blockchain Voting: The End To End Process, https://followmyvote.com/blockchain-voting-the-end-to-end-process/ (consultado el 02/07/2019)

[7] Bokslag, W., de Vries, M. Evaluating e-voting: theory and practice. arXiv preprint arXiv:1602.02509, 2016.

[8] Busaniche, B. Heinz, F., Rezinovsky, A., *Voto Electrónico. Los riesgos de una ilusión*, Fundación Vía Libre, Córdoba, 2008.

[9] Busaniche, B., *Voto electrónico: Una solución en busca de problemas*, Fundación Vía Libre, Córdoba, 2017.

[10] Chaum, D. “Blind signatures for untraceable payments”. Advances in Cryptology - Crypto '82, Springer-Verlag pp. 199-203, 1982.

[11] Chaum, D. “Security Without Identification: Transaction System to Make Big Brother Obsolete”. Communications of the ACM, v. 28, n. 10, pp. 1030-1044, 1985.

[12] Chaum, D. “Untraceable electronic mail, return addresses and digital pseudonyms”. Communications of the ACM, v. 24, . pp. 84-88, 1981.

[13] Chaum, D., Carback, R., Clark, J., Essex, A., Popoveniuc, S., Rivest, R., Ryan, P., Shen, E., Scantegrity II: End-to-end verifiability by voters of optical scan elections

through confirmation codes. IEEE Transactions on Information Forensics and Security, 4(4):611–627, 2009.

[14] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A., Vora, P. Scantegrity: End-to-end voter-verifiable optical-scan voting. Security & Privacy, IEEE, 6(3):40–46, 2008.

[15] Chaum, D., Sherman, A., Fink, R., Carback, R., Scantegrity III: Automatic Trustworthy Receipts, Highlighting Over/Under Votes, and Full Voter Verifiability. In Proceedings of the 2011 conference on Electronic voting technology/workshop on trustworthy elections EVT/WOTE'11, USENIX Association Berkeley, CA, 2011.

[16] Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg, 1991.

[17] Civitas: A Secure Voting System,
https://www.cs.cornell.edu/projects/civitas/ (consultado el 14/05/2019)

[18] Díaz Pace, J., “Análisis de la factibilidad de la implementación de tecnología en diferentes aspectos y etapas del proceso electoral”, Consejo Nacional de Investigaciones Científicas y Técnicas, 2017.

[19] ElGamal, T. “A public key cryptosystem and a signature scheme based on discrete logarithms”. CRYPTO’ 84, Springer-Verlag, LNCS 196, pp.10-18, 1984.

[20] Helios Voting,
https://heliosvoting.org/ (consultado el 26/07/2019)

[21] Meter, C., "Design of Distributed Voting Systems." arXiv preprint arXiv:1702.02566. 2017.

[22] Morales Rocha, V., “Seguridad en los procesos de voto electrónico remoto: Registro, votación, consolidación de resultados y auditoría”. Universitat Politècnica de Catalunya, 2009.

[23] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system, 2008.
https://bitcoin.org/bitcoin.pdf (consultado el 02/07/2019)

[24] Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System,
https://eprint.iacr.org/2013/214.pdf (consultado el 26/05/2019)

[25] Scantegrity Whitepaper,
http://scantegrity.org/papers/whitepaper.pdf (consultado el 14/05/2019)

[26] Schneider, A., Meter, C., Hagemeister, P., ”Survey on Remote Electronic Voting”, arXiv preprint arXiv:1702.02798, 2017.

[27] Shamir, A., *How to share a secret*. Communications of the ACM 22,11 pp. 612-613, 1979.

[28] STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System, https://www.usenix.org/system/files/conference/evtwote13/jets-0101-bell.pdf (consultado el 19/05/2019)

[29] The Pret a Voter Verifiable Election System, https://web.archive.org/web/20101128061130/http://www.pretavoter.com/publications/PretaVoter2010.pdf (consultado el 19/05/2019)

[30] TIVI - Verifiable Voting, https://www.smartmatic.com/fileadmin/user_upload/Factsheet_TIVI.pdf (consultado el 02/07/2019)

[31] Xiaojun, Wen. An E-payment system based on quantum group signature. Physica Scripta. 82. 065403. 10.1088/0031-8949/82/06/065403, 2010.