ANÁLISIS DE FACTIBILIDAD EN LA IMPLEMENTACIÓN DE TECNOLOGÍA EN DIFERENTES ASPECTOS Y ETAPAS DEL PROCESO ELECTORAL

CONICET

Octubre de 2017

CONICET

CONSEJO NACIONAL DE
INVESTIGACIONES CIENTÍFICAS Y TÉCNICAS
Godoy Cruz 2320, Buenos Aires - 011 4899-5000

PRESIDENTE DEL CONICET

Dr. Alejandro Ceccatto

COMISIÓN ASESORA

El análisis e investigación que dio por resultado el presente documento fue realizado por una Comisión Asesora integrada por:

Coordinación Técnica

Jorge Andrés Díaz Pace – ISISTAN - Investigador independiente

Dante Zanarini - CIFASIS -Miembro del grupo de investigación: "Fundamentos y aplicaciones de la lógica y la programación" y Profesor Adjunto UNR

Miembros

Iván Arce – ICC – Investigador Asociado

Maximiliano Cristiá -CIFASIS - Director del Grupo de Ingeniería de Software de CIFASIS

Pablo Mandolesi - IIIE - Investigador Adjunto

Hernán Melgratti – ICC - Investigador Adjunto

Gustavo Uicich – ICYTE- Investigador

Nicolás Wolovick - UNC - Profesor Adjunto

Eduardo Zavalla - INAUT - Investigador

Agradecimiento por la participación de Federico Bergero - CIFASIS - Investigador Asistente

GESTIÓN DEL PROYECTO

El proyecto se gestionó a través de la Gerencia de Organización y Sistemas del CONICET

Coordinación

Diego Asensio – Gerente de Organización y Sistemas

Edición

Lorena Carlino – Coordinadora del Repositorio Institucional CONICET Digital

CONTENIDO

Análisis de factibilidad en la implementación de tecnología en diferentes aspectos y etapas del proceso electoral 5

1. Objetivos y Contexto 5
2. Alcance 7
3. Modelo de Referencia 10
4. Principios de Construcción 11
5. Antecedentes 16
6. Evaluación Técnica 20
7. Consideraciones para el Desarrollo/Selección de Hardware 31
8. Consideraciones sobre el Proceso de Desarrollo de Software 38
9. Conclusiones y Recomendaciones 44

REFERENCIAS 47

ANEXO: Escenarios de Calidad 51

ANÁLISIS DE FACTIBILIDAD EN LA IMPLEMENTACIÓN DE TECNOLOGÍA EN DIFERENTES ASPECTOS Y ETAPAS DEL PROCESO ELECTORAL

1. Objetivos y Contexto

Este documento tiene por objeto realizar un *análisis de factibilidad* de un sistema de voto electrónico que contempla a la boleta única, a requerimiento del *Ministerio del Interior, Obras Públicas y Vivienda, Presidencia de la Nación* (MI). Este análisis implica la investigación de distintas soluciones técnicas, con distintos grados de automatización del proceso de votación y riesgos asociados, a fin de proveer información y fundamentaciones para la toma de decisiones por parte del MI.

Por boleta única se entiende un artefacto oficial impreso (por ej., en papel) en el que figura la oferta electoral completa (las opciones electorales), el cual es distribuido solamente en el sitio oficial de la votación. Las boletas únicas son marcadas por los votantes (en el lugar de votación) para emitir su voto, y deben ser mantenidas en secreto.

El desarrollo de un sistema de voto electrónico es complejo no sólo por sus desafíos técnicos, sino también por su importancia para el Estado y para la sociedad en general. Un sistema de voto electrónico involucra la consideración de aspectos de software, hardware, procesos operativos, y personas. En este sentido, cualquier desarrollo debe atender el aspecto de calidad del sistema como un objetivo esencial del proceso de construcción.

Específicamente, el MI ha planteado los siguientes objetivos para el sistema de votación a considerar:

- Garantizar la completitud en la oferta electoral.
- Simplificar el uso de boletas (por ej., con una boleta única).
- Brindar mayor accesibilidad a los ciudadanos a la hora de votar (por ej., para personas con alguna discapacidad).
- Lograr precisión y rapidez en el proceso de conteo de votos.

Se considera también que un sistema de votación, y especialmente uno que incorpore algún grado de automatización, tiene entre sus objetivos construir la confianza de los ciudadanos, partidos políticos y gobierno, en el sistema y en el proceso de votación.

Además del MI, se identifican otros interesados del sistema (*stakeholders*) a saber:

- Votantes (ciudadanos).
- Autoridades de los comicios.
- Partidos políticos.
- Proveedores del proceso electoral.
- Otros poderes del Estado, entre los que se pueden mencionar poderes legislativo, ejecutivo y provinciales.

Desde la perspectiva de estos interesados, surgen distintas propiedades a satisfacer, tales como:

- Secreto del voto: a excepción del sufragante nadie debe poder tener conocimiento alguno del contenido del voto; incluso existiendo eventualmente colaboración del sufragante, la veracidad del contenido del voto revelado no debe poder demostrarse. No sólo debe garantizarse esta propiedad, sino que su validez debe ser evidente para cualquier votante. De otra manera, la sola sospecha de que alguien pueda conocer el contenido de su voto impide la libre emisión del sufragio.
- Integridad: se define en tres partes:
    1. Capturar la intención de voto de manera fehaciente (y sin introducir sesgos)
    2. Registrar la intención de voto exactamente como fue capturada
    3. Contabilizar el voto exactamente como fue registrado.

    La propiedad de integridad del sistema requiere garantizar que la cadena de confianza, involucrando las tres componentes anteriores, no puede romperse.
- Capacidad de *auditoría* y control del proceso electoral (sin afectar los atributos de secreto e integridad anteriores).
- Igualdad de condiciones para todos los partidos políticos.
- Universalidad en el sentido de permitir que todos los ciudadanos habilitados puedan ejercer el voto (incluso personas con requerimientos de accesibilidad, por ej., no videntes).
- Convalidación: análisis post-hoc del proceso electoral.
- Usabilidad: Debe ser usable y adecuado a las capacidades de los votantes, las autoridades electorales, fiscales partidarios, y toda persona afectada al sistema.

Además, un sistema de votación debe cumplir con las normativas vigentes del proceso electoral.

Todas estas características conducen a atributos de calidad técnicos que deben ser incorporados al evaluar alternativas de solución.

Por otro lado, es preciso mencionar que existen antecedentes previos de distintos sistemas de voto electrónico, tanto en otros países como en Argentina, los cuáles constituyen una base de experiencias y conocimiento valioso para sustentar el presente informe.

El resto del documento se estructura en nueve secciones. La Sección 2 define el alcance del análisis realizado, y presenta los principales atributos de calidad técnicos considerados para el sistema. La Sección 3 considera un modelo de referencia desagregado en fases para un sistema de votación con boleta única. La Sección 4 enuncia una serie de principios de construcción que son aplicables a los sistemas de votación, y que condicionan posibles soluciones derivadas del modelo de referencia. La Sección 5 resume distintos antecedentes de soluciones de voto electrónico en otros países. La Sección 6 realiza una evaluación de los posibles peligros que podrían surgir en cada una de las fases del modelo, en base a las fuentes de información relevadas. La Sección 7 presenta algunas consideraciones importantes referidas a la selección del hardware para un sistema de votación, mientras que la Sección 8 presenta consideraciones para el proceso de software. Finalmente, la Sección 9 resume las conclusiones del estudio, y brinda ciertas recomendaciones de la Comisión Asesora para una implantación criteriosa del modelo propuesto.

2. Alcance

El análisis de factibilidad está basado en requerimientos funcionales generales para un sistema de voto electrónico, y particularmente en requerimientos no funcionales (o de atributos de calidad) que se consideran claves en este tipo de sistemas. El análisis no tiene por objetivo proveer una especificación funcional detallada, ni una solución concreta al problema, sino presentar un panorama de opciones con distintos grados de factibilidad.

Los requerimientos funcionales para sistemas de votación han sido relevados en distintos proyectos y artículos, y sirven como referencia para orientar el presente análisis (Has & Ryan, 2017). Ciertamente, estos requerimientos específicos dependen del grado de automatización de la solución a considerar y aunque son necesarios, se considera que la

satisfacción de los requerimientos de atributos de calidad es crítica en un sistema de votación. Se consideran relevantes los siguientes atributos de calidad (Bass, Clements & Kazman, 2012) (aunque no todos se abordaron con el mismo nivel de detalle):

- **Usabilidad:** qué tan fácil es para un usuario del sistema (de votación) realizar cierta tarea, y cómo resulta el tipo de soporte brindado a sus usuarios (por ej., accesibilidad, uso eficiente del sistema, confianza, satisfacción, o bajo impacto de errores, entre otros).
- **Seguridad:** capacidad del sistema para proteger datos e información de accesos no autorizados, pero proveyendo al mismo tiempo acceso a personal autorizado para operar. En particular, se consideran importantes las propiedades de confidencialidad, integridad, disponibilidad y autenticidad.
- **Auditabilidad:** capacidad de monitorear el sistema tanto en su diseño (estructura), como cuando se encuentra en funcionamiento (ejecución) y cuando ya dejó de utilizarse (análisis a-posteriori). En un sistema de votación debe poderse auditar todos los niveles de hardware y software.
- **Verificabilidad:** habilidad para demostrar que un sistema (o programa de software) ha sido construido y se comporta de acuerdo con sus especificaciones. En el caso de sistemas de votación, este atributo tiene una connotación particular, mediante la propiedad de verificación punta-a-punta (Benaloh et al., 2013).
- **Desempeño:** capacidad del sistema para cumplir eficazmente con sus especificaciones. Como ejemplo, para un sistema de votación puede considerarse el tiempo necesario para computar los resultados en el escrutinio provisorio.
- **Escalabilidad:** posibilidad de despliegue y operación del sistema con el agregado de múltiples recursos computacionales, de manera que este crecimiento le permita funcionar eficientemente (por ej., un sistema de votación por ciudad que se expande luego a un contexto provincial, o incluso nacional).
- **Confiabilidad:** capacidad del sistema para evitar estados o condiciones que puedan causar problemas o daños a ciertos actores del ambiente de operación del software (por ej., votantes, fiscales, etc.). En algunos casos, es deseable que ante estos estados o condiciones el sistema pueda recuperarse.
- **Robustez:** capacidad del sistema de tener alternativas para cumplir con el resultado. Una forma de lograrlo es mediante la incorporación de redundancia con modos de fallo independientes para que en caso de que el sistema principal falle, el sistema secundario o terciario pueda suplantarlo.

Es preciso considerar que los atributos de calidad son “no operacionales”, lo cual significa que un mismo atributo puede tener distintas interpretaciones en distintos contextos (del mismo sistema), o en distintos sistemas, o cuando son considerados por distintos *stakeholders*. Por esta razón, es necesario trabajarlos en este análisis mediante instancias concretas denominadas *escenarios*. También se debe considerar que muchas veces estos atributos entran en contraposición unos con otros, esto se conoce como punto de compromiso (Kulyk, Neumann, Budurushi, & Volkamer, 2017, Bass, Clements & Kazman, 2012). Ejemplos típicos de puntos de compromiso pueden ser: desempeño versus seguridad, o seguridad versus usabilidad, entre otros.

Por otra parte, debido al escaso tiempo disponible para el análisis, se decidió dejar fuera de consideración ciertos aspectos del problema que requieren una investigación más profunda. De cualquier manera, las conclusiones presentadas son independientes de estos aspectos. Los aspectos fuera de alcance son los siguientes:

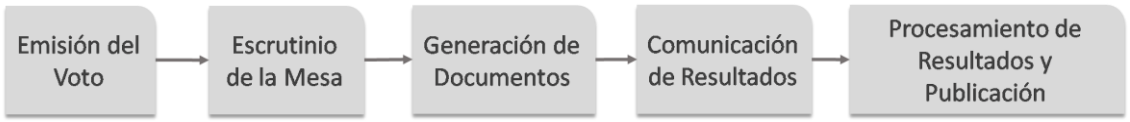
- No se analizó el sistema de votación actual con que cuenta el país. Se asumió que tiene falencias y que el MI desea solucionarlas incorporando tecnología informática. Aun así, es preciso remarcar que vale la pena analizar también soluciones no informáticas a los problemas actuales, dada la complejidad y riesgos inherentes[1].
- No se estudiaron en detalle las implementaciones de voto electrónico existentes en el país ni las usadas en otros países. Por el contrario, el análisis se centró en cuestiones generales sobre las ventajas, dificultades y peligros asociados al uso de tecnología informática para este tipo de sistemas. Es indudable que, si se decidiera incorporar tecnología en una solución concreta, se deberán analizar con detalle las soluciones existentes.
- No se efectuó un análisis formal de riesgos. Se considera que esta actividad requiere de mayor tiempo, y el análisis de riesgos debería efectuarse sobre una solución concreta.
- No se tuvieron en cuenta contramedidas a ciertos ataques o fallas que podrían darse en un sistema de votación electrónica. Nuevamente, esta tarea depende en gran medida de la implementación concreta que se considere.

[1] Consultado en: http://www.cij.gov.ar/nota-26851-La-C-mara-Nacional-Electoral-fij--pautas-para-la-asignaci-n-de-fondos-p-blicos-para-la-impresi-n-de-boletas.html

- No se trabajó sobre aspectos de Interfaz de Usuario (UI) y Experiencia de Usuario (UX) que resultan importantes a la hora de mostrar la oferta electoral y su proceso de selección ya que pueden producir sesgo. Incluso debería analizarse si una UI resulta efectivamente más sencilla que una boleta papel de una o más páginas.
- No se estudiaron los aspectos legales, normativos, políticos, ni sociales de una solución informática.
- Se consideró la implementación de un modelo "de referencia" para voto electrónico (ver Sección 3) simplemente por conveniencia para el estudio del problema. Sin embargo, si se considera la posibilidad de que existan múltiples implementaciones y se usen simultáneamente, la interoperabilidad e interacciones entre ellas, es un factor que debe estudiarse en profundidad.
- No se incluyeron en el análisis los sistemas relacionados con la gestión de padrones electorales, ni con la identificación del votante durante el acto electoral.
- No se incluyen en el análisis procesos y actividades relacionadas con el escrutinio definitivo. Se advierte que un cambio en el sistema de votación podría requerir una adecuación del procedimiento de escrutinio definitivo.

3. Modelo de Referencia

El problema de la votación en un contexto de Escrutinio Provisorio (EP) se puede conceptualizar en términos de cinco fases secuenciales, según se esquematiza en la siguiente figura. Estas fases son relevantes al presente análisis, ya que cada una de ellas representa una "unidad" del proceso susceptible de ser automatizada. Las fases están derivadas del Código Electoral Nacional (Decreto N° 2135, 1983).



1. **EMISIÓN DEL VOTO**. Comprende la votación propiamente dicha de cada ciudadano, en la cual éste expresa su preferencia electoral dentro de la oferta y luego emite su voto (tradicionalmente depositándolo en la urna).
2. **ESCRUTINIO DE LA MESA**. Al cierre del acto eleccionario, en cada mesa se realiza el escrutinio y suma de los votos, la cual es realizada por la autoridad de mesa, bajo la supervisión de los fiscales partidarios. Actualmente, este conteo se efectúa manualmente.

3. **GENERACIÓN DE DOCUMENTOS**. Como resultado del conteo de votos, la autoridad de mesa completa una serie de documentos (por ej., actas de escrutinio, certificados electorales, o telegramas de escrutinio) que reflejan los resultados de cada mesa. Actualmente, estos documentos se trabajan en un soporte físico (papel).
4. **COMUNICACIÓN DE RESULTADOS**. Los resultados del escrutinio se transmiten al centro de procesamiento de datos (por ej., los documentos en papel se envían vía fax a la Dirección Nacional Electoral del Ministerio del Interior).
5. **PROCESAMIENTO DE RESULTADOS Y PUBLICACIÓN**. El centro de procesamiento de datos recibe los diferentes resultados, ingresa y consolida la información y anuncia públicamente los resultados provisorios.

Tal como se menciona en la Sección 2, estas fases secuenciales asumen que, antes de emitir su voto, cada ciudadano se ha identificado adecuadamente ante la autoridad de mesa respecto al padrón.

Es preciso considerar que, por simplicidad, en el modelo de referencia presentado se omiten dos actividades requeridas en la ley relativas a la confección de las actas de apertura y de cierre de urnas. Las distintas alternativas para las fases que se analizan en este documento podrían afectar la manera en que dichas actividades deberían ser llevadas a cabo. Esto requiere ser analizado de acuerdo a la solución que se adopte.

4. Principios de Construcción

El hardware y software que implementa cualquiera de las fases en las que se ha dividido el proceso de votación pertenecen a la categoría de *sistemas de misión crítica (o mission-critical software-reliant system)*, debido principalmente a los atributos de calidad en juego y a la reducida ventana de operación donde el sistema debe funcionar “casi sin fallas” *(*Axelrod, 2012 y U.S. Election Assistance Commission, 2017*)* . El desarrollo se vuelve aún más sensible en caso de considerar la automatización de la fase de emisión del voto.

En general, un sistema se considera de misión crítica si uno o más de sus elementos constitutivos (por ej., componentes de software, componentes de hardware, personal, procesos) son esenciales para la continuidad del negocio de una organización, y una falla o disrupción en alguno de estos elementos puede impactar seriamente en los objetivos del sistema. Estos sistemas son frecuentes en industrias tales como la aeroespacial,

aerocomercial, automovilística, de dispositivos médicos, ferroviaria (incluyendo trenes subterráneos), tarjetas inteligentes, o de energía nuclear.

De acuerdo a Saltzer & Schroeder (1975) los aspectos de Seguridad Informática cobran gran importancia en un sistema de misión crítica ya que, en este caso en particular, un error en el sistema que pueda ser explotado por un atacante podría atentar contra algunos de los principios básicos del voto o el resultado de la votación en general. Por tal motivo, el desarrollo del hardware y software debe estar sujeto, como mínimo, a los principios de construcción para sistemas de misión crítica. Además, dado el carácter social y político del sistema de votación de un país, el hardware y software que se desarrollen o utilicen para tal fin deben poder ser auditados por los ciudadanos y las instituciones.

En base a estas consideraciones, se enuncian y discuten a continuación una serie de principios de construcción, ya sean provenientes de sistemas de misión crítica o generalmente aceptados para el desarrollo de sistemas de votación. El objetivo de estos principios es servir como guías y restricciones para el análisis posterior. En la medida que se sigan estos principios y se apliquen desde etapas tempranas de la construcción, mayor será la calidad del sistema resultante.

Todo el desarrollo debe ser abierto (*open source* y de carácter público) Según Montes, Penazzi, & Wolovick (2016) y Norris (2004) el código fuente del sistema debe estar disponible al público en general, y toda la documentación generada durante el desarrollo también debe ser pública. Esta documentación incluye diseños, arquitectura y especificaciones del software y el hardware, planes de verificación de ambos, minutas de las reuniones del equipo de desarrollo, pruebas efectuadas sobre el hardware y el software y sus resultados, contratos con proveedores y fabricantes de componentes críticos, entre otros artefactos. Además, es recomendable que tanto el código fuente como la documentación estén disponibles desde el “minuto cero”, y no solamente luego de que se haya finalizado el desarrollo del sistema. Por ejemplo, el código fuente puede estar disponible (para consulta) en un repositorio de acceso público, que permita que el ciudadano pueda escrutar el sistema y reportar errores, omisiones, etc. desde el inicio del proyecto. Si el código fuente u otra documentación solo se libera una vez terminado el desarrollo, resulta mucho más difícil y costoso corregir errores. En general, este principio soporta los atributos de *Auditabilidad, Verificabilidad y Seguridad*. Más aún, luego de que el sistema se haya terminado, el público deberá contar con un tiempo razonable para auditar el sistema (en este contexto, “razonable” se corresponde normalmente al orden de meses).

El sistema debe ser demostrablemente correcto. Según Rivest (2008) y Appel (2016) el sistema debe ser construido de forma tal que demostrar su corrección sea relativamente simple. En este sentido, la simplicidad de la prueba de corrección debe ser uno de los objetivos del desarrollo. Esto implica utilizar componentes que hayan sido previamente certificados (por ej., mediante pruebas formales mecanizadas); utilizar técnicas de diseño y arquitectura de software que tiendan a generar componentes pequeños, simples y bien definidos; utilizar diseños estándar; documentar la especificación y el diseño del sistema utilizando notaciones al menos semi-formales; evitar el uso de lenguajes de programación cuya semántica no esté debidamente documentada; evitar las construcciones de lenguajes de programación que impliquen esfuerzos de verificación costosos (por ej., la aritmética de punteros); entre otras. Como consecuencia, no se deben implementar mecanismos de seguridad que hagan uso de técnicas de *seguridad por oscuridad*. Según Scarfone, Jansen, & Tracy (2008) este tipo de seguridad refiere a que ésta depende del secreto de la implementación de uno o más de sus componentes. Este principio da soporte mayormente a los atributos de *Seguridad* y *Verificabilidad*.

El fabricante/proveedor debe ofrecer una prueba de corrección del sistema. Dado el carácter de misión crítica del sistema de votación, el proveedor debe suministrar una prueba de la corrección del sistema, la cual debe incluir una prueba de su seguridad. Es decir, no basta con enunciar que el sistema es correcto y seguro, sino que debe proveer evidencia contundente que respalde dichas afirmaciones (ISO/IEC 15408, 2009). Este principio da soporte a los atributos de *Verificabilidad* y *Seguridad.*

El sistema que debe proporcionar el fabricante/proveedor debe ser de alta disponibilidad. El fabricante deberá proveer argumentos técnicos convincentes que indiquen que se han tomado medidas para que el sistema funcione durante todo el comicio, o en su defecto existan *planes de contingencia* adecuados. Esto se debe a que, según el Código Electoral Nacional, una vez iniciada la elección esta no puede ser interrumpida, y si lo fuera por razones de fuerza mayor se expresará en acta separada el tiempo que haya durado la interrupción y la causa de ella (Art. 99). En particular, el proveedor deberá demostrar que ha considerado todas las fallas evidentes/razonables/probables en la solución que provea, que ha estudiado cómo se detectarán esas fallas, que ha evaluado la posible frecuencia de esas fallas, que ha documentado debidamente los procedimientos que indican qué se debe hacer ante cada falla, que ha calculado cuál es el tiempo promedio para continuar operando luego de cada falla, y que ha capacitado al personal interviniente acerca de cómo actuar ante cada falla, entre otros. Este principio da sustento al atributo de *Confiabilidad* y *Robustez*.

El sistema de votación debe ser independiente del software. Es ampliamente conocida la dificultad de la industria del software para *garantizar* el correcto funcionamiento de sus productos, y en particular, para construir sistemas que resistan ataques informáticos. Por tal motivo, es necesario que el sistema de votación responda al principio enunciado por Rivest (2008) denominado *software independence* que indica que un cambio o error no detectado en el software no pueda producir un cambio o un error no detectado en el resultado de la elección. Este principio no implica que el software no tenga errores, sino que si los tiene, sus efectos sobre el resultado de la elección deben ser notorios. Por ejemplo, un sistema que al ser atacado no transmite los resultados de una mesa al centro de cómputos verifica este principio, puesto que existe un reaseguro (por ej., los fiscales, las actas en papel y el escrutinio definitivo) que hará evidente el problema. El principio rector es que "las elecciones deben dar una evidencia consistente de un resultado preciso, aun cuando el rival sea quien escribe el software, administra la elección o gobierna el país" (Benaloh, Ryan, Schneider & Teague, 2017). Este principio soporta los atributos de *Auditabilidad* y *Verificabilidad*.

Debe incluir un sistema de contingencia que no dependa del hardware ni del software utilizado en el sistema principal. Nuevamente apelando al carácter crítico del sistema y dado que es imposible garantizar la inexistencia de eventos que lo corrompan, debe preverse la existencia de un sistema de respaldo apropiado tal como proponen Swanson, Bowen, Phillips, Gallup, & Lynes (2010) . Este sistema de respaldo debe ser tal que se puedan poner en acción partes de él sin tener que iniciarlo de forma completa. Por ejemplo, si el sistema principal incluye el uso de impresoras, debe contemplarse la posibilidad de que una de ellas falle y por lo tanto considerarse su reemplazo (individual) por otra impresora o por un mecanismo equivalente (por ejemplo, manual). Este principio soporta los atributos de *Confiabilidad y Robustez*.

La seguridad del sistema debe depender de la menor cantidad posible de hardware y software. Cuanto menor sea la cantidad de hardware y software involucrada en la implementación de los mecanismos de seguridad, menos son las posibilidades de existencia de errores (Saltzer & Schroeder, 1975). En consecuencia se reducen las posibilidades de ataques y fallos. La reducción en la cantidad de hardware y software para este fin aumenta las posibilidades de realizar una verificación rigurosa (e incluso formal) de los componentes críticos del sistema. Observar que el sistema puede utilizar más hardware y software siempre y cuando éste no sea responsable de la seguridad del sistema. La verificación de estos componentes puede no ser tan rigurosa. Este principio contribuye a los atributos de *Seguridad* y *Verificabilidad*.

Específicamente para sistemas de votación (sea en formato de papel o electrónicos), se ha demostrado formalmente que existe una tensión o compromiso entre los atributos de integridad, auditabilidad y privacidad, y más aún, que existe una imposibilidad de satisfacer perfectamente los tres atributos en forma simultánea (Hosp & Vora, 2008). Este teorema influye significativamente en los cuatro principios subsiguientes.

El sistema debe preservar el secreto del voto. Es insospechada y contra-intuitivamente difícil preservar un secreto guardado en un sistema de cómputo. Aun así, el voto debe permanecer confidencial (secreto). Por esta razón, el proveedor deberá utilizar el repertorio de técnicas conocidas por la comunidad de Seguridad Informática para garantizar tal propiedad (en particular, se consideran relevantes los trabajos académicos sobre el problema de la confidencialidad en sistemas de cómputo). Este principio es heredado de la condición de voto secreto.

El sistema no puede ni debe identificar al votante. Si el sistema permite identificar al votante, se disminuye notablemente la posibilidad de garantizar el secreto del voto. La identificación del votante debe realizarse en forma independiente del sistema de emisión de voto. En consecuencia, este principio desaconseja los sistemas que requieran la lectura de la huella digital, cualquier otro dato biométrico o la utilización de algún código individual, para permitir usar la máquina de emisión de votos (Montes, Penazzi, & Wolovick, 2016).

El sistema debe preservar la integridad del voto. Preservar la integridad del voto significa garantizar que se respeta la voluntad de cada votante, es decir que el sistema no permita cambiar el voto una vez que el votante lo emitió. En particular, el fabricante debe suministrar una prueba de que esta propiedad se verifica.

El sistema debe preservar la integridad del resultado de la votación. Preservar la integridad del resultado de la votación significa que si el sistema, por error o ataque, altera la suma de los votos individuales lo hará de una forma que será evidente para los ciudadanos. Por lo tanto, el fabricante debe suministrar una prueba de que esta propiedad se verifica.

No composicionalidad. En base a trabajos como los de Sutherland et al. (1991), Zakinthinos & Lee (1998), Mantel, Sands, & Sudbrock (2011) y Mantel (2002), se ha comprobado que el sistema que resulta de la constitución de componentes que verifican cierta propiedad de seguridad, no necesariamente verifica la misma propiedad. Por este motivo, la composición de las fases descritas en la Sección 3 en un sistema integrado debe analizarse como un todo (y no únicamente analizar los componentes

individualmente). En consecuencia, se desaconseja efectuar tal integración sin extremar las prácticas de desarrollo seguro y la verificación del sistema. El principio de no composicionalidad también puede aplicarse a otros atributos de calidad del sistema.

Auditabilidad. El desarrollo de la solución debe ser abierto (*open source* y de acceso público). Debe considerarse un proceso de desarrollo con revisiones permanentes y auditorías formales sobre los distintos artefactos. Estas auditorías no sólo evaluarán el software y el hardware, sino también los procedimientos, planes de contingencia, contratos con proveedores, especificaciones, pruebas de corrección, técnicas de verificación y validación utilizadas, *test suites* utilizados y el análisis de cobertura de estos, entre otras cosas. Dado que la introducción de cualquier modificación al sistema auditado, invalida las presunciones sobre el nivel de riesgo del sistema, el mismo no deberá modificarse entre la última auditoría y su puesta en producción.

Estos puntos refuerzan la idea de que el proceso de adopción de esta tecnología debe ser llevados a cabo con la antelación suficiente que permita asegurar el cumplimiento de los objetivos planteados.

Cualquier ciudadano, universidad u organización civil debe poder analizar el sistema electoral sin necesidad de ser convocado expresamente para ello. Este requerimiento introduce un potencial conflicto de intereses para las auditorías, los que deberán ser considerados, así como las pautas de resolución oportunamente establecidas.

Los procesos de auditorías y los resultados de las mismas deberán ser públicos, para reforzar la confianza de la ciudadanía en su sistema electoral.

Dado que el proceso eleccionario tiene recurrencia, una forma de mejorarlo es evaluar el uso de la técnica cada vez que se utiliza. El estudio post hoc garantiza el continuo crecimiento y mejoramiento de los procesos bajo el análisis de los resultados.

5. Antecedentes

En esta sección se analizan experiencias de estudio/adopción de alternativas de voto electrónico en distintos países. Este análisis no pretende ser exhaustivo, sino ilustrar la complejidad del proceso de adopción de voto electrónico en distintas partes del mundo, así como también las dificultades encontradas y las vulnerabilidades detectadas en dispositivos de voto electrónico.

El estudio se focaliza principalmente en aquellas experiencias relacionadas con la adopción de alternativas de voto electrónico presencial. En concordancia con el alcance

del estudio de factibilidad planteado, las experiencias relacionadas con la implementación de mecanismos para posibilitar elecciones electrónicas de manera remota (*Internet voting*) no serán analizadas.

Estados Unidos: El uso de dispositivos de votación en Estados Unidos cobró especial relevancia a partir del año 2000, luego de las elecciones presidenciales en donde un gran número de votos no fueron registrados apropiadamente (*residual votes*). Estudios subsiguientes como los de Brady, Buchler, Jarvis, & McNulty (2001) y de Kimball, Owens, & McAndrew Keeney (2002) mostraron que los mecanismos de votación con tarjetas perforadas tenían un gran número de votos residuales. Como solución a los problemas evidentes de los sistemas de tarjetas perforadas, comienza el auge de los dispositivos de registro electrónico directo de votos (DRE[2]) (Brady & Hui, 2008). No obstante, estos sistemas han sido ampliamente cuestionados, debido a razones fundamentales sobre su incapacidad para garantizar la verificabilidad de los resultados y sus vulnerabilidades, tal como lo manifiestan Bannet, Price, Rudys, Singer & Wallach (2004), Mercuri (2001) y Jacobs & Pieters (2009). En consecuencia, se impulsa la adopción de sistemas acompañados por dispositivos de registro en papel que sea verificable por los usuarios (VVPAT). Asimismo, el uso de estos dispositivos han recibido muchos cuestionamientos respecto a su usabilidad (Everett, 2007 y Bederson, Sherman, Herrnson & Niemi, 2003), robustez y seguridad (Bannet, Price, Rudys, Singer & Wallach, 2004). Los sectores científicos y académicos abogan por el desarrollo de sistemas de votación que permitan verificación punto a punto (*end-to-end verifiable voting*), pero tales sistemas aún se encuentran en etapas embrionarias y su usabilidad es cuestionada (Acemyan, Kortum, Byrne, & Wallach, 2014 y Winckler et al., 2009).

Actualmente, en los distintos estados se emplean diferentes sistemas, que a menudo son utilizados combinadamente. Es preciso considerar que en la actualidad hay debates sobre los dispositivos utilizados, y existen causas judiciales en muchos estados respecto a su uso, en Mercuri[3] (2017) se resumen estos casos.

Paralelamente, en 2002 se aprueba la ley federal *Help America Vote Act*, que establece un organismo de control denominado *Election Assistance Commission* (EAC). El EAC conforma un comité técnico para delinear recomendaciones guías para los sistemas de votación. Este comité comenzó su actividad en Julio de 2004 y elaboró un primer

[2] DRE del inglés: *Direct-recording electronic*

[3] Consultado en: http://www.notablesoftware.com/evote.html

documento: *Voluntary Voting System Guidelines* (VVSG 2005), con lineamientos guías en Abril de 2005. Sin embargo, posteriormente recomendó reemplazar el documento VVSG 2005 por otro que considere en profundidad aspectos de seguridad, testing de usabilidad y establecimiento de estándares y métodos de prueba para sistemas de votación electrónica. En 2009, se produce una revisión incremental de VVSG 2005 (la versión 1.1) que aún no ha sido adoptada.

La versión VVSG 2.0, que reescribe completamente la recomendación VVSG 2005, estableciendo criterios y requerimientos para sistemas que, por ejemplo, incluyen VVPAT, se entregó en agosto 2007 (Technical Guidelines Development Committee, 2007). El comité técnico se encuentra aún trabajando en aspectos que mejoran esta recomendación, pero la misma no se ha implementado aún.

En 2007, la EAC comenzó el proceso de certificación de equipamiento de voto electrónico, respecto de la versión VVSG 2005. Además esta comisión lleva registro de distintos problemas reportados sobre los dispositivos que se usan en la actualidad (*Voting System Reports* Collection[4], 2017).

Holanda: este país ha sido pionero en la adopción del voto electrónico. En 1965 aprobó el uso de máquinas para la emisión del voto (incluidas a las electrónicas) y a partir de la década de los 90 se promovió la adopción de equipamiento DRE (Jacobs & Pieters, 2009). Sin embargo, en mayo de 2008 el gobierno decidió retornar al voto en papel con conteo manual, como conclusión a un proceso de desconfianza creciente sobre las garantías que proveían las computadoras de votación, y que pueden resumirse principalmente en dos puntos según definen Jacobs & Pieters (2009) y Loeber (2008):

- Oscurantismo del sistema y falta de verificabilidad: código y resultados de auditorías secretos. El código estaba protegido por derechos a la propiedad del proveedor. Imposibilidad de acceder al sistema para evaluarlo.
- Muestras de vulnerabilidades al sistema: un grupo logró tener acceso a los dispositivos y mostraron varias vulnerabilidades del sistema, como por ejemplo:
    - Facilidad para alterar el comportamiento del sistema, permitiendo modificar el conteo o hacer que la computadora ejecute cualquier código.

[4] Consultado en: https://www.eac.gov/voting-equipment/voting-system-reports-collection/

- Sujeto a *Tempest attack*: la pantalla de la computadora emitía radiaciones que podían ser utilizadas para reconstruir su estado, y posibilitando violar el secreto del voto.

Cabe destacar que existía una especificación en la legislación holandesa de los requisitos para el sistema de votación y un proceso de auditoría independiente que debía certificar la adherencia del sistema implementado. Sin embargo, un aspecto importante evidenciado en Gonggrijp et al. (2006) ha sido que los sistemas analizados satisfacían los requerimientos enunciados por la ley, sin embargo los mismos admitían implementaciones altamente inseguras.

Previo a retomar el voto en papel y recuento manual se solicitó a dos comisiones de expertos la evaluación independiente. Como puntos principales de las conclusiones de estos trabajos pueden mencionarse:

- Escaso control de gobierno en el proceso eleccionario, que dependía en gran medida del proveedor que diseñaba y testeaba el sistema;
- Falta de verificabilidad. Una comisión recomendó la incorporación de un registro en papel (tipo VVPAT) o mecanismo equivalente (pero no precisado). La segunda desaconsejó mantener registros duplicados, dado que son fuentes de inconsistencias, y proponía separar las fases de votación y conteo, usando una impresora y un scanner. Para avanzar en esta dirección se analizó la construcción de una impresora de votos que evite el problema del *tempest attack*, sin embargo, no se encontró una solución satisfactoria a este problema.
- Ventajas competitivas a ciertos candidatos (el "candidato 31" de la lista).

Alemania: Alemania comenzó a utilizar dispositivos electrónicos de voto (en realidad DRE Nedap utilizados en Holanda) a partir de 1998, comenzando con pruebas pilotos en Colonia y sucesivamente adoptados en distintas ciudades, y generalmente bien aceptadas por la ciudadanía, hasta 2005. En ese año, un par de ciudadanos presentaron una causa ante la Corte Constitucional Alemana, alegando que el uso de máquinas de votación electrónica es inconstitucional y que, dado que son vulnerables, los resultados de las presidenciales de 2005 no son confiables. Un fallo de esta corte dictaminó que el uso de las máquinas Nedap es inconstitucional, dado que la legislación alemana requiere que los pasos de la elección puedan ser validados por la ciudadanía, algo que no es posible con las máquinas empleadas. Aunque este fallo no prohíbe el uso de cualquier

dispositivo electrónico, sino que requiere que los mismos sean transparentes, hoy Alemania usa la boleta única en papel[5].

Brasil: En 2002 Brasil implementó una elección a escala nacional utilizando unos 406.000 dispositivos electrónicos en la cual más de 100 millones de votantes emitieron su sufragio. La tecnología utilizada es de dispositivos de registración directa (DRE). Los reportes de testing de seguridad públicos en 2012 muestran que existen problemas técnicos severos en los dispositivos utilizados (Aranha, Karam, de Miranda, & Scarel, 2014). Se menciona que la mayoría de las medidas de protección adoptadas apuntan a lograr ofuscación y no seguridad. Entre los problemas más relevantes se señalan la inadecuada protección del secreto del voto, el uso inapropiado de encriptación y algoritmos de criptografía obsoletos, modelos de ataques inadecuados centrados en atacantes externos cuando los ataques internos presentan un riesgo mucho mayor, adopción de un proceso de desarrollo de software defectuoso (malas prácticas y proceso inmaduro) y verificación de integridad insuficiente.

Existen otros países cuyas experiencias en la adopción de sistemas de voto electrónico es también importante analizar. Entre ellos, se puede mencionar India, Venezuela, Israel, Filipinas e Irlanda. Los resúmenes de cada caso no se incluyen en el documento con el fin de mantener un adecuado balance en la presentación.

Específicamente, no se ha analizado la implementación de sistemas de voto electrónico en Argentina, con el fin de evitar posibles sesgos en el análisis y se ha preferido basar el estudio en experiencias internacionales de las cuales se cuenta con información académica u oficial.

6. Evaluación Técnica

En esta sección se realiza una evaluación de posibles riesgos y factibilidad técnica de las cuatro primeras fases del modelo de referencia, en base a la consideración de distintas fuentes de información: los atributos de calidad, los principios de construcción, los antecedentes de otros países, y la experiencia de los miembros de la Comisión. Se ha decidido realizar un análisis de cada fase en un “orden inverso”, comenzando por la fase que se considera menos riesgosa de implementar en el corto plazo, y continuar

[5] Consultado en: https://www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany

progresivamente hasta llegar a la fase inicial considerada la más riesgosa y que por lo tanto requiere esfuerzos a largo plazo.

El análisis de atributos de calidad sigue una metodología basada en *escenarios* (Babar & Gorton, 2004). Para cada atributo de calidad, se han generado distintos escenarios que capturan aspectos concretos del atributo. Cada escenario puede afectar una o más fases del modelo de referencia. La finalidad de la lista de escenarios generados para cada fase no es exhaustiva, sino que pretende investigar “casos testigos” a partir de los cuales los expertos identifican riesgos (o peligros) asociados a la fase. Algunos de estos escenarios se presentan en el Anexo.

Adicionalmente, para cada fase se analiza la adherencia a los principios de construcción. La criticidad (o nivel de riesgo) global de cada fase se determina en función de los riesgos pertinentes a la fase y del grado de compromiso a los principios de construcción.

En este contexto, se definen los siguientes niveles de criticidad en base a un código de colores:

 no se han identificado riesgos o compromisos en el sistema.

 los principios fundamentales del voto no se encuentran comprometidos, aunque existen riesgos (menores) de diferencias en el resultado provisorio que luego pueden ser corregidas en el escrutinio definitivo.

 existen riesgos moderados de alterar el resultado de la elección, sin que esto pueda ser detectado y/o corregido.

 existe un alto riesgo de comprometer los principios fundamentales del voto y de alterar de forma indetectable el resultado de la elección.

Es preciso considerar que los niveles de criticidad solamente consideran cada fase en forma individual; atendiendo al principio de no-composicionalidad, el riesgo o criticidad de una fase puede incrementarse si se decide automatizar la fase precedente. Por ejemplo, si se incorpora tecnología a la fase de emisión de voto, entonces la fase de escrutinio de la mesa incrementa sensiblemente su nivel de riesgo al incorporarse tecnología también en esta etapa.

6.1. Comunicación de Resultados

Para esta etapa se asume que se cuenta con un telegrama de escrutinio firmado (al menos) por la autoridad de mesa. Es posible que dicho documento tenga además un soporte digital conteniendo la misma información que se encuentra impresa.

A fin de evitar demoras en la transmisión de telegramas, es factible realizar su digitalización y transmisión desde el mismo local de votación (Poder Judicial de la Nación[6], 2017)

Desde el punto de vista de la confiabilidad y verificabilidad del sistema, estos atributos aumentan si se transmite la imagen del documento, además de la información contenida en el soporte digital. De esta manera, si se publica tanto el resultado como la imagen del telegrama, cualquier ciudadano podrá contrastar la información y detectar posibles inconsistencias entre lo impreso y lo digital.

La autenticidad e integridad de la información a transmitir son propiedades fundamentales que deben garantizarse. La confidencialidad de los datos no es tan relevante en esta fase, puesto que es información que debe hacerse pública en el menor lapso de tiempo posible, atendiendo al atributo de desempeño. Esta situación refleja un punto de compromiso en el diseño, en el cual lo principal es preservar la integridad del resultado de la votación.

Disponer de un soporte digital en el documento evita la carga manual de los datos en el centro de procesamiento. Además, al recibirse la imagen del telegrama y los datos en formato digital, el resultado de la mesa puede ser publicado directamente sin intervención humana. Sin embargo, esta opción debe evaluarse con sumo cuidado, puesto que si la integridad de los datos fue afectada (es decir, el formato digital no coincide con lo impreso) o se dan otras situaciones anómalas (por ej., el telegrama no está firmado por la autoridad de mesa, o no se distinguen los números impresos), la confiabilidad del sistema puede verse afectada.

Una solución *de compromiso* al problema descrito en el párrafo anterior puede alcanzarse incorporando un proceso de validación de los datos, que controle cuestiones de forma (por ej., presencia de firmas) y que contraste la imagen del telegrama impreso con los datos digitales del mismo. En caso de existir coincidencia, los datos pueden publicarse. Si difieren, puede enviarse a las autoridades respectiva para su consideración. De esta

[6] Consultado en: https://www.pjn.gov.ar/cne/documentos/2017%20AE%20003-17%20(ESCRUTINIO%20PROVISORIO).pdf

forma, se evita la carga manual de datos en el centro del procesamiento, pero se mantiene un proceso de validación sobre la información.

Además de los riesgos asociados al punto de compromiso entre desempeño y confiabilidad (integridad), se deben considerar los riesgos derivados del software de transmisión, el cual debe ser auditado. Adicionalmente, es deseable contar con un plan de contingencia para casos de indisponibilidad en las líneas de comunicación. La inclusión de puntos de control (humanos) en un proceso automatizado permite mitigar riesgos, aunque estos puntos de control pueden introducir demoras de desempeño en el cómputo de los resultados del escrutinio.

En resumen, se considera que la incorporación de tecnología a esta fase es factible, y puede mejorar el desempeño en el proceso de escrutinio, e incluso ciertos aspectos del proceso operativo actual. Si bien existen riesgos en esta fase, los mismos pueden ser mitigados, y en última instancia no afectan el resultado del escrutinio final, ya que los votos ya han sido emitidos y contabilizados en cada mesa.

6.2. Generación de Documentos

De acuerdo al modelo de referencia, esta etapa comienza una vez que se dispone del resultado del escrutinio en la mesa. Al finalizar, se cuenta con la siguiente documentación:

- Actas de escrutinio, firmadas por las autoridades de mesa y fiscales presentes.
- Certificados de escrutinio, firmados por el presidente de mesa.
- Telegrama de escrutinio, firmado por las autoridades de mesa y fiscales presentes.

Entre las alternativas para esta etapa, se puede mencionar la confección manual de estos documentos, o la asistencia digital para la confección y posterior impresión de los mismos. Es preciso considerar que, de acuerdo a la legislación vigente, las actas y certificados deben ser generados en papel, mientras que los datos a transmitir no necesariamente deben ser volcados a soporte papel.

En caso de introducir tecnología en esta etapa, se debe proveer al presidente de mesa de un dispositivo para realizar la carga de los datos, así como también de un medio de impresión de documentos. Ambos dispositivos podrían estar o no integrados. Asimismo, si el proceso de conteo se realizó con asistencia tecnológica, es posible que los datos ya se encuentren digitalizados, y por lo tanto sólo deba proveerse un medio de impresión. En términos de usabilidad y desempeño, una ventaja de esta solución es que permite al

sistema realizar chequeos básicos de consistencia (por ej., que todos los datos necesarios estén presentes, o que la suma de los votos coincida con el total de votantes).

Por otro lado, si el resultado del recuento se introduce una única vez, entonces la información presente en los documentos de escrutinio será la misma. De esta manera, se evitan situaciones en las cuales el contenido de un documento no coincide con el de otro (esta clase de errores es frecuente en el esquema actual, pues el presidente de mesa transcribe varias veces los mismos datos). Por último, se supone que un documento impreso de forma digital resulta más legible que uno manuscrito.

Los dispositivos de software a utilizar deben adherir al principio de independencia de software. Es preciso considerar que en esta etapa es fundamental preservar la integridad de la información, mientras que no es relevante garantizar su confidencialidad, dado que los actores involucrados ya conocen el resultado y este sólo debe llevarse a soporte papel. Este punto de compromiso es similar al analizado para la fase de transmisión de resultados.

Por otro lado, es imprescindible asegurar la disponibilidad del sistema, teniendo en cuenta que los documentos de escrutinio son parte fundamental del proceso electoral. Una falta de disponibilidad del software puede afectar negativamente el desempeño en el proceso de cómputo del escrutinio. Es por eso que debe aplicarse aquí el principio de contar con planes de contingencia.

Una alternativa que impacta positivamente en las siguientes etapas es la de generar, junto a la documentación impresa, un soporte digital para los datos. Esto facilita la posterior transmisión y procesamiento de los resultados. Sin embargo esta opción introduce riesgos, pues se tendrá la misma información en dos soportes diferentes. Es por eso que, bajo esta alternativa, debe tenerse especial recaudo a fin de preservar la integridad: los formatos impresos deben coincidir con los digitales. El soporte digital puede estar presente en el documento (por ej., mediante un chip o un código QR), o se puede optar por transmitir directamente los resultados desde el dispositivo de carga de datos. Esta última alternativa se percibe como más riesgosa, dado que un potencial error de inconsistencia entre el soporte papel y el digital será detectado luego de publicarse el resultado de la mesa. Además, deberá evaluarse el impacto en la *confianza* del sistema, si sólo se publican los datos del resultado, pero no las copias digitalizadas de los telegramas.

En caso de incorporarse soporte digital a los documentos, es importante publicar la forma en que se almacenan los datos, así como toda la información necesaria para la

interpretación independiente de los mismos. De esta manera, los fiscales que así lo deseen podrían validar la coincidencia entre los formatos impresos y los digitales, utilizando para ello sus propios dispositivos de lectura (por ej., un lector de códigos QR en un *smartphone*).

En términos de auditabilidad, la solución a implementar debe proveer los mecanismos necesarios para que los actores involucrados en esta etapa (autoridades de mesa y fiscales) puedan validar, previo a la firma del documento, que los formatos impresos coincidan con el resultado del recuento. También deben contemplarse planes de contingencia que permitan, si la circunstancia lo requiere, transitar esta etapa sin asistencia tecnológica. Por ejemplo, se puede habilitar la generación manual de los documentos en caso de falla del sistema.

En resumen, se considera que la incorporación de tecnología es factible, pudiendo realizar aportes en el desempeño de la generación de documentos y en una mayor oportunidad de verificación (o fiscalización) por parte de los partidos políticos. No obstante, se observan riesgos asociados a la integridad de los documentos, ya que los formatos impresos pueden no coincidir con los formatos digitales, y la detección de estas diferencias puede darse luego de que se haya publicado el resultado provisorio de la mesa. Este tipo de riesgo no es fácil de mitigar, aunque no afectaría el resultado del escrutinio definitivo. También se destacan ciertos riesgos respecto a la disponibilidad del sistema.

6.3. Conteo

El conteo corresponde a la fase del proceso electoral donde se totalizan los resultados por categoría y partido político. En el sistema electoral es el presidente de mesa el único encargado de realizar esta totalización bajo el escrutinio de Fiscales Partidarios. El circuito electoral requiere que cada mesa realice un recuento independiente y auditado que será plasmado en una o más actas con la misma información.

Es posible incorporar tecnología para asistir al proceso de conteo de votos a través de técnicas de Visión por Computadoras que tienen una tasa de fallos razonablemente baja cuando se realiza sobre medios pensados para este fin, como es el sistema de boleta única con marcas. Es preciso considerar que aunque actualmente, las técnicas de visión por computadora son más precisas que los humanos, también existen ataques para aumentar la tasa de fallos al nivel que se desee, sin siquiera modificar el software de reconocimiento de imágenes (Appel, 2016).

Esto implica una vez más que **la computadora deberá ser un asistente en el conteo** y que su resultado sea tomado como una primera aproximación. El resultado final plasmado en las actas será el obtenido por el conteo manual realizado por el presidente de mesa y tal vez re-asegurado por el conteo automático. De esta forma, se tiene un **mecanismo robusto de conteo** que es compatible con el principio de independencia del software. Si el conteo automático funciona bien, sirve para cotejar con el sistema manual y ganar confianza; si el conteo automático falla en alguna de sus múltiples formas (por ej., no llegaron las computadoras, las computadoras no arrancan, se rompió el scanner, el software está adulterado, etc.) el conteo manual lo suplanta.

Resulta importante remarcar que el procedimiento que se realice impida a los presidentes de mesa tomar el resultado arrojado por las computadoras y trasladarlo automáticamente a las planillas y telegramas. Se recomienda estudiar estrategias para mitigar este problema, aprovechando que se está ante un problema *de independencia del software*, como por ejemplo realizar *risk limiting audits* a posteriori (Hall et al., 2009). Es preciso considerar también como un potencial problema que ante la detección de fallas, estas se produzcan luego de que la opinión pública haya aceptado un resultado.

La experiencia internacional marca algunas pautas claras acerca de los procedimientos para llevar adelante la incorporación de tecnología en esta etapa.

- Uso de Boleta Única con marcas (condados de Estados Unidos de Norteamérica, Holanda, Alemania).
- Marcas que solo sean reconocidas si se hacen con el sello y tinta especial provista por el CNE (Korean Elections: A Model of Best Practice - The Asia Foundation [7], 2017).

En resumen, se considera que el conteo electrónico ayuda a las autoridades de mesa a generar confianza en el resultado del conteo, siempre y cuando se asegure el principio de independencia de software, y esto es básicamente la verificación efectiva de que la cuenta manual coincide con la cuenta electrónica, ya sea obligando a hacer el conteo manual o realizando *risk limiting audits* a posteriori.

Si la emisión de votos se realiza con soporte de computadoras, entonces el nivel de riesgo actual de la fase de conteo conlleva riesgos adicionales, sobre todo respecto a la anonimidad del voto. Además, si no se asegura que se contabilice manualmente, la composición de estos dos sistemas podría ser equivalente a contar con un DRE.

[7] Consultado en: http://asiafoundation.org/2016/04/20/korean-elections-a-model-of-best-practice/

Vale aclarar que, para elecciones o distritos electorales con pocas categorías, el **conteo electrónico** no será necesariamente ni más rápido ni más preciso que el manual, pero sí extremadamente más caro. Este punto debe ser evaluado a priori a fin de valorar si el despliegue de tecnología en cada mesa resulta eficiente.

6.4. Emisión de Voto

La Emisión de Voto es la fase del proceso electoral en la que el ciudadano habilitado para votar expresa y registra su intención de voto. Cuando un dispositivo electrónico intermedia entre el votante y el registro de su intención de voto, el sistema electoral incluye un sistema electrónico para la emisión del voto, lo que popularmente se llama “voto electrónico”. Los atributos de calidad referidos a un sistema de emisión de voto son: universalidad del voto, garantías de la oferta electoral, integridad (con sus 3 aspectos), confidencialidad, y usabilidad, según se describió en la Sección 1.

Los requerimientos enunciados en la Sección 1 para un sistema electrónico para la emisión del voto son distintivos en el campo de las TIC, debido a los múltiples puntos de compromiso existentes en las propiedades que se requiere satisfacer simultáneamente en este sistema. Es preciso observar, por ejemplo, que los sistemas de transacciones financieras no imponen requerimientos de anonimidad sobre quienes los usan ni disocian a cada usuario de las operaciones que realiza. La dificultad técnica, y que distingue al proceso de votación de otros sistemas informáticos, es que el requerimiento de mantener el secreto — que implica que un voto no puede ser asociado a su emisor— imposibilita luego explicar si un voto fue emitido válidamente por un votante o el mismo es consecuencia de un mal funcionamiento del software (Jacobs & Pieters, 2009). Esta limitación no se debe meramente a fallas en el diseño de los sistemas conocidos, sino que hay una demostración teórica de que tres de las propiedades requeridas (integridad, auditabilidad y secreto) son mutuamente excluyentes y no se pueden satisfacer completamente de manera simultánea (Hosp & Vora, 2008).

El requerimiento de garantizar el secreto del voto es fundamental en esta fase, y se traduce en un conjunto de requerimientos no funcionales equivalentes sobre el sistema, los cuales fueron enunciados como principios en la Sección 4. En particular, **el sistema no debe**:

- Filtrar ni la intención ni el registro del voto a un tercero, al momento de la emisión ni en ningún momento posterior de manera tal que se puedan asociar votos con votantes. Esto no debe ser posible incluso si se tiene control parcial o completo

del sistema de emisión del voto (por ej., por su fabricante o un proveedor o algún actor que los controle o infiltre).

- Permitir que un tercero pueda determinar de manera inequívoca a quien votó un votante, incluso si puede ejercer coerción sobre él o si cuenta con su cooperación.
- Permitir que un tercero pueda determinar de manera inequívoca que un votante no votó a un candidato determinado. Nótese que, en una elección con más de dos opciones, este requerimiento no es equivalente al anterior.

Debido a varios problemas técnicos (por ej., canales encubiertos) es muy complejo garantizar el secreto del voto, y proveer evidencia de que tal propiedad se cumple (Lampson, 1973. Goguen & Meseguer, 1982. Sutherland et al., 1991. Klein et al., 2009). En consecuencia, esto implica un esfuerzo meticuloso y sostenido, que requiere de personal altamente calificado y largos tiempos de desarrollo. El sistema resultante de tal esfuerzo podrá cumplir parcialmente algunas de las propiedades que se le requieren. Adicionalmente, todo esfuerzo dirigido a garantizar el cumplimiento estricto de las propiedades de integridad y secreto del voto va en detrimento de la verificabilidad y auditabilidad del sistema, en la medida que incrementan la complejidad y sofisticación de la técnica empleada.

En consecuencia, cualquier sistema de emisión electrónica de voto que busque solucionar los problemas inherentes a garantizar integridad y secreto, necesariamente será difícil de verificar formalmente y de auditar, incluso por expertos en la disciplina.

No existe evidencia en la actualidad de que sea factible utilizar un dispositivo electrónico en esta fase del proceso de votación sin comprometer requerimientos fundamentales del voto, en particular, garantizar el secreto.

A esto hay que agregar que un sistema para la emisión del voto implica un alto riesgo, ya que está expuesto a todos los votantes habilitados, las autoridades de mesa y todo el sistema logístico del acto electoral. En una elección de escala nacional o incluso provincial, es un sistema distribuido de misión crítica en el que una falla (en todos, o en un gran número de “nodos”) puede ser catastrófica (por ejemplo, puede producir demoras, o incluso detener o suspender la elección).

A continuación se analizan algunas de las realizaciones más representativas de sistemas de emisión de voto electrónico (Has & Ryan, 2017):

- *Direct-recording electronic* (DRE) *voting machine*. Con estos dispositivos los electores pueden emitir su voto a través de medios mecánicos o electrónicos

(típicamente botones o pantalla táctil) y cada voto es procesado por un programa que lo registra en memoria. Al cierre de la urna, cada DRE provee los resultados del escrutinio de acuerdo con los votos almacenados. Adicionalmente pueden proveer funcionalidades para la transmisión y consolidación de datos.

- DRE + *Voter Verifiable Paper Audit Trail* (VVPAT): Son dispositivos DRE que cuentan con mecanismos de confirmación al votante acerca del voto que va a ser emitido. Típicamente los VVPAT muestran al votante una versión impresa del voto que va a ser emitido y que puede ser comprendida por el usuario. Este registro impreso se almacena como comprobante del voto emitido. Los resultados del escrutinio se obtienen electrónicamente en función de los votos registrados electrónicamente por el DRE y los comprobantes quedan disponibles para realizar auditorías o para recuento en caso de controversia.
- *Electronically-assisted ballot marker* (EBM) y *Electronic Ballot Printers* (EBP): Estos dispositivos asisten a los votantes en la emisión de votos presentando las opciones electorales en una pantalla electrónica y cuando el votante finaliza su elección, imprimen un voto en papel. Estos dispositivos no deben guardar registro electrónico de los votos emitidos.
- *End-to-End Verifiable Voting System* (E2EVV): Estos dispositivos permiten al usuario realizar su elección a través de una pantalla electrónica e imprimir un registro en papel de una versión encintada del voto emitido, que conserva el votante. Este comprobante puede ser utilizado en la máquina para verificar visualmente o probando a la máquina que el voto fue registrado de acuerdo a la elección del votante. Al cierre de los comicios, el sistema hace públicos todos los votos emitidos, por ejemplo en la Web. De esta manera cada votante puede confirmar que su voto fue registrado correctamente (es decir, su comprobante se encuentra dentro del lote de votos registrados por el sistema). El escrutinio se realiza efectuando computaciones criptográficas que permiten obtener el resultado de la elección.

Cuando se utilizan sistemas de registro directo de votos sin registro físico (DRE) es imposible verificar los resultados del sistema de votación (Mercuri, 2001, Jacobs & Pieters, 2009). En respuesta, se han propuesto DRE alternativos que generan comprobantes físicos a través de la impresión en papel de los votos de los usuarios (VVPAT o *Verifiable Paper Record*), que introducen otras vulnerabilidades al sistema de votación.

Los sistemas que emiten un comprobante físico (EBM, EBP o DRE+VVPAT) permiten la realización de ataques adicionales contra el secreto del voto, por ejemplo, si utilizan un

identificador único a un voto o cualquier otra característica funcional que permita distinguir un voto emitido de otro. Esto puede ocurrir de diferentes maneras. Por ejemplo, se pueden incluir chips RFID que llevan un identificador único, o mantener el orden en que fueron emitidos los votos, como en el caso de DRE+VVPAT con cinta de papel continua. Adicionalmente, el software que controla la emisión del voto puede agregar información sobre el momento o el orden de emisión del voto no detectable por el votante (esteganografía) que permita a un tercero vulnerar el secreto. Los registros físicos con contenido no decodificable visualmente por el votante (por ej., uso de QR o chip RFID) son aún más vulnerables.

Otros ataques que vulneren el secreto del voto se pueden realizar aprovechando las características físicas del soporte que se utilice. Por ejemplo, se ha mostrado que es posible leer a distancia el voto en casos de implementaciones que incluyen chips RFID (Oren & Wool, 2010).

Los sistemas de doble registro, por ejemplo, DRE+VVPAT o impresión de boletas con información textual más QR o RFID, generan peligros adicionales sobre la integridad de los resultados debido a que pueden obtenerse distintos resultados a partir de las diversas fuentes. Por ejemplo, si se utilizara un recuento automático de boletas impresas utilizando un lector QR, la integridad del sistema podría ser vulnerada haciendo que la información textual (que puede verificar una persona) difiera de la información codificada, que será finalmente la utilizada en el conteo.

Existen cuestionamientos sobre la efectividad de los sistemas con registro en soporte físico (o de impresoras de votos) para garantizar que los votos sean emitidos de acuerdo con la voluntad del votante. El supuesto principal en el diseño de estos sistemas es que el votante controlará el voto emitido por el sistema. Estudios que evalúan el comportamiento de los usuarios frente a estos sistemas muestran que una proporción alta de los usuarios (50 a 65%) no controla que el voto emitido se corresponda con su elección (Everett, 2007 y Campbell & Byrne, 2009). Esto disminuye la probabilidad de detectar que el sistema haya sido vulnerado (por ej., si de manera aleatoria o estadística genera un comprobante distinto al elegido).

El uso de un dispositivo, con o sin registro en papel, al momento de emisión del voto introduce oportunidades de ataque contra el secreto del voto, como por ejemplo:

- *Tempest attack* (caso Holanda).

- Dispositivos de emisión con capacidad de cómputo/memoria/comunicación que podrían registrar información adicional sobre el orden o momento de emisión que atentan contra el secreto del voto.

La emisión del voto mediada por un dispositivo electrónico puede afectar también requerimientos relacionados con garantizar la completa oferta electoral no sesgada. Diseños inadecuados podrían introducir sesgos (a favor o en contra) al momento de presentar la oferta electoral, como en el caso holandés del “candidato 31”. Además, el sistema podría no garantizar una completa oferta electoral en todo momento, sesgando la misma en función del horario, localización geográfica o cualquier otra variable que permita influir en el resultado de la elección.

Desperfectos o mal funcionamiento del sistema (corrupción en la emisión del sufragio o en la oferta electoral) pueden impedir el derecho de emitir sufragio. En este caso, la disponibilidad del sistema cobra relevancia, y hace necesario contar con planes de contingencia.

Se debe considerar que los riesgos de ataques aumentan si se permite la interacción no monitorizada con el dispositivo de emisión del voto (por ej., implementando un cuarto oscuro). Este es un punto de compromiso con alternativas para minimizar ataques contra el secreto del voto.

En resumen, se desea remarcar el alto riesgo de utilizar computadoras en esta fase, debido al requerimiento de garantizar el secreto del voto, el cual entra en contraposición con requerimientos de auditabilidad e integridad. Las alternativas existentes para la emisión de voto con dispositivos plantean distintos grados de compromiso, pero aún así no resuelven los problemas analizados. Una excepción son los sistemas de tipo E2EVV, que si bien tienen el potencial de resolver estos problemas, se encuentran todavía en un estadío de desarrollo académico y son cuestionables desde el punto de vista de la usabilidad y escalabilidad. Se debe considerar también que los problemas o errores que puedan introducirse en esta fase (detectables o no) se pueden propagar a las siguientes fases del modelo, y esto eleva el nivel de riesgo de todo el sistema.

7. Consideraciones para el Desarrollo/Selección de Hardware

A fin de consolidar las consideraciones que resultan de utilidad para la evaluación de la mejor opción de hardware para cada fase, se analizan a continuación un conjunto de aspectos que llevan a distintos compromisos y que deben ser resueltos efectivamente.

Capacidad. El equipamiento debe disponer de todas las capacidades necesarias para la ejecución de la función a realizar.

Disponibilidad. La disponibilidad del equipamiento para la tarea se encuentra amenazada por la posible ocurrencia de una o más fallas y/o ataques, las que provocan que el dispositivo no pueda ser utilizado. El mecanismo de análisis de fallas de los equipos a utilizarse es una elección compleja, que debe tener como finalidad predecir el comportamiento lo más fielmente posible bajo la tipología de uso que reciba el equipamiento. En este sentido gran parte de las técnicas utilizadas buscan elaborar análisis de la vida media y predicción de fallas. En el caso de equipamiento para el proceso de votación, el uso del mismo es por eventos, lo que se asimila más al análisis de sistemas **"one shot"** que al de los equipos comerciales. Para asegurar la disponibilidad, conociendo el modelo de fallas se deben realizar procesos y disponer de equipamiento redundante.

Otro factor clave en la disponibilidad es la existencia de energía. En este caso el análisis de riesgo debe considerar el espacio físico donde se instalarán las máquinas, o en su defecto proponer la independencia de las mismas del sistema eléctrico. En este último caso la máquina sigue teniendo como insumo la energía y su disponibilidad estará sólo afectada por la falla propia del sistema o por fallas en el suministro propio.

Vulnerabilidad. Esta propiedad identifica la capacidad de lograr una variación en el comportamiento especificado del equipo. Este es el caso en que la operación de la máquina no produce el resultado esperado, ya sea por modificaciones de su lógica interna o por alteración de su hardware o software si lo tuviere. Estas variaciones no están contempladas en el modelo de fallas del análisis de disponibilidad y pueden dar lugar a nuevos peligros no analizados.

Observabilidad. Es la potencial interpretación del estado interno de la máquina por parte de toda entidad ajena a la persona que la está operando. Estos peligros atentan contra el secreto del voto y se deben a la existencia de **"canales ocultos"** que pueden ser correlacionados con la operación. Los canales más comunes son los introducidos por el EMI (*Electro Magnetic Interference*) radiado, el conducido por los cables de alimentación, el ruido producido por los elementos mecánicos y/o la temperatura.

Integridad. La integridad del equipamiento está relacionada a la capacidad de acceso al mismo por personas no designada para manipularla sin tener un fin legítimo. En este caso resultan vitales las medidas y procedimientos de custodia, de almacenamiento, de traslado y de posterior resguardo de los equipos.

Orientación del Hardware. En este caso se visualizan dos opciones muy diferenciadas: *Hardware dedicado* y *Hardware de propósito general*, y el abordaje de cada una de las opciones es completamente diferente.

Se considera que las características físicas y constructivas de los sistemas electrónicos (*hardware*) dedicados al proceso de votación asistida deben diseñarse específicamente para la función que deben ejecutar, en contraposición al posible uso de hardware de propósito general (computadoras tipo PC o similares). Es decir, se considera que debe priorizarse en términos de reducción de vulnerabilidades, el uso de *software específico* ejecutado por *hardware específico* en lugar de *software específico* ejecutado en *hardware genérico*.

En el caso del *hardware dedicado* se debe concretar un diseño en base a los requerimientos específicos de ejecución e incluir las mejores técnicas de diseño que permitan mitigar los riesgos existentes.

En el caso de *hardware* de propósito general el análisis es más complejo en virtud de las innumerables configuraciones y conectividades disponibles, y debe estudiarse la incorporación de medidas y hardware complementario que fortalezcan al equipo ante los conflictos del problema.

En relación al modelo de referencia definido en la Sección 3, se entiende asimismo que resulta conveniente que se defina un hardware diferenciado y específico asociado a cada una de las etapas del proceso, de manera de desacoplar las vulnerabilidades individuales y mejorar las posibilidades de auditar su funcionamiento. De este modo, deberían utilizarse tres tipos diferentes de sistemas de hardware respectivamente para las etapas de: a) emisión de voto, b) recuento de votos, y c) generación de documentos y comunicación de resultados; en la medida en que esta separación no traiga aparejados nuevos peligros que requieran contramedidas adicionales para su mitigación. Se recomienda que cada uno de los sistemas de hardware a desarrollar deben ser construidos por diferentes fabricantes.

Atendiendo a los principios de auditabilidad y verificabilidad, se sugiere que los diagramas esquemáticos circuitales y firmware sean de verificación pública. Asimismo, el hardware final debe ser verificable por entidades técnicas, partidos políticos, otros poderes del estado, organizaciones no gubernamentales y ciudadanos en general. El sistema debe someterse a análisis con suficiente antelación para ejecutar ensayos que cuestionen cada componente de hardware. Toda incidencia, alcance y variación debe reportarse con un análisis detallado en forma abierta.

Si bien no se define en este documento un conjunto de especificaciones técnicas a cumplir por cada uno de ellos, es posible realizar recomendaciones generales en función de cada fase:

a. Etapa de Emisión del Voto

En esta etapa y como resultado de la interacción del ciudadano votante con la máquina de emisión de voto (MEB) se supone que se produce una boleta o recibo en papel u otro material de soporte, con la representación de la voluntad del voto de dicho ciudadano.

Algunos de los peligros identificados en relación al hardware son los siguientes:

- La Máquina Emisora de Boletas (MEB) se daña y no puede brindar servicio.
- La MEB es manipulada electrónicamente para modificar la representación del voto.
- La MEB es manipulada para almacenar y/o transmitir información adicional sobre la interacción del votante con la misma, que pueda ser utilizada posteriormente para asociar al elector con su voto.
- La MEB es manipulada para sesgar el modo de presentación de la oferta electoral.
- La MEB es reemplazada por hardware ilegítimo no distinguible por los usuarios.

En este contexto, un hardware de MEB debe tener un diseño y construcción robusta, debiendo resistir manipulaciones maliciosas y vandalismo. Asimismo, debe ser fácil de transportar y de rastrear en caso de extravío, condiciones que no se cumplen en computadoras de uso estándar. Éstas últimas, a su vez, proveen una innumerable conectividad a dispositivos externos, lo que, sumado a la incorporación de un sistema operativo genérico, atenta contra la resistencia a la manipulación.

A continuación, se enuncian aspectos técnicos mínimos que deberían ser considerados respecto del hardware para un dispositivo de emisión de votos.

- No debe tener capacidad de almacenamiento estático (disco rígido, SSD, flash NVRAM, CMOS RAM con supercapacitor, etc.)
- El software debe ser de acción mínima y almacenable en *Read Only Memory - One Time Programmable* (ROM OTP). Se debe reemplazar por hardware dedicado la mayor funcionalidad posible.
- Los componentes deben ser completamente inaccesibles, quedando solo disponible la interfaz del usuario a comandar por hardware y el ingreso de carga para cumplir su función.
- En previsión de posibles canales encubiertos el sistema de hardware debería:

  - Filtrar toda conexión a la red eléctrica para evitar comunicaciones PLC (*Power Line Carrier*). Se prefiere en cambio operación a baterías, duplicada en capacidad de energía como alternativa de respaldo, desmontables para garantizar desenergización.
  - No poseer memoria flash ni otro tipo de memoria no-volátil accesible en ejecución.
  - Montarse sobre un sistema de blindaje que garantice un campo eléctrico radiado que sea inferior a los niveles detectables inmersos en el ruido eléctrico de un ambiente periurbano.
  - Contar con un mecanismo de hardware que evite la introducción de marcas o caracteres espurios en la boleta, abriendo potencialmente canales de información encubiertos.
  - Impedir el acceso con tecnología de uso masivo a los soportes WORM, si se decidiera por el uso adicional de este tipo de soporte para acelerar la lectura de datos en la etapa de conteo (por ejemplo RFID o código QR óptico).
  - Agregar ruido no correlacionado con el funcionamiento interno si la máquina no fuera silenciosa

- La arquitectura debe contar con separación física (por hardware) entre memoria de datos y memoria de instrucciones de proceso (programa).
- El sistema de alimentación de la memoria RAM debe garantizar que se extingue el contenido de la misma al apagado de la máquina.
- Los sistemas de autodestrucción ante eventos no autorizados requieren mayoritariamente de una fuente de energía adicional *on-board*, que es preferible evitar para garantizar la volatilidad de información al apagado.
- El diseño del *hardware* debe tener como características que un intento de alteración conlleve la destrucción del mismo (por ejemplo el PCB -*Printed Circuit Board*) podría embeberse en epoxi u otro material de bajo índice de contracción al curado, pero con fuerte adherencia al PCB para evitar la remoción de componentes).
- En el caso de usar partes comerciales, debe evitarse la identificación de partes con el fin de ser usado en el dispositivo. Por ejemplo, el microcontrolador a usar tiene que proceder de un fabricante con volumen de venta elevado en relación a la cantidad de máquinas a construir (~100k) (Texas, Atmel, NXP, etc.) y debería adquirirse en distribuidores (al menos 3 diferentes), no directamente a fábrica.
- Debe evitarse el acceso no seguro a los puertos de programación.

b. Etapa del Conteo de Votos

En esta etapa las autoridades de mesa, debidamente identificadas, realizan la cuenta de los votos extraídos de la urna, asistidos por la Máquina de Conteo de Votos (MCV) ante la vista de fiscales.

Algunos de los peligros identificados en relación al hardware son los siguientes:

- La MCV no está operativa.
- La máquina MCV es manipulada para cambiar su comportamiento o dañarla irreversiblemente.

Los requisitos deberían seguir un patrón de diseño similar al de MEB dado que los riesgos son similares. Estos requisitos se mencionan a continuación:

- La MCV no debería poseer puertos de comunicación cableados o inalámbricos accesibles desde el exterior de la carcasa o incluso desmontando ésta, a excepción del puerto destinado a la descarga de la oferta electoral para la homologación de los votos emitidos.
- En previsión de posibles canales encubiertos el sistema de hardware debería filtrar toda conexión a la red eléctrica para evitar comunicaciones PLC (*Power Line Carrier*). Se prefiere en cambio operación a baterías, duplicada en capacidad de energía como alternativa de respaldo, desmontables para garantizar desenergización.
- La MCV debe contar con mecanismos de seguridad para evitar la descarga de datos que no contengan firma digital autorizada.
- La MCV debe contar con separación física (por hardware) entre memoria de datos y memoria de instrucciones de proceso (programa).
- El PCB podría embeberse en epoxi u otro material de bajo índice de contracción al curado, pero con fuerte adherencia al PCB para evitar la remoción de componentes y mejorar la performance térmica.
- El conjunto podría montarse sobre un sistema de blindaje que garantice inmunidad a un ataque electromagnético moderado.
- En el caso de usar partes comerciales, debe evitarse la identificación de partes con el fin de ser usado en el dispositivo. Por ejemplo, el microcontrolador a usar tiene que proceder de un fabricante con volumen de venta elevado en relación a la cantidad de máquinas a construir (~100k) (Texas, Atmel, NXP, etc.) y debería adquirirse en distribuidores (al menos 3 diferentes), no directamente a fábrica.

- El fabricante de la MEB debe ser diferente al fabricante de la máquina de conteo de votos (MCV).

c. Etapa de Generación de Documentos y Comunicación de Resultados

Al final del proceso, la Máquina de Generación de Documentos (MGD) genera aquellos documentos que reflejan el resultado de la votación en cada mesa y los transmiten para su consolidación.

Algunos de los peligros identificados en relación al hardware son los siguientes:

- Alteración de documentos electrónicos en tránsito.
- La MGD no está operativa.
- La MGD no puede generar o imprimir los documentos.
- No es posible enviar los documentos electrónicos.

En esta etapa los riesgos inherentes están relacionados con el mecanismo de transmisión, por ello las máquinas que transfieren los documentos electrónicos no están sujetas a restricciones de seguridad tan estrictas como en las etapas anteriores. De todas maneras, se deben procurar las siguientes condiciones:

- La MGD no debería poseer puertos de comunicación cableados o inalámbricos accesibles desde el exterior de la carcasa o incluso desmontando ésta, a excepción de los que se deben utilizar para la transmisión segura de los datos.
- La MGD debe contar con separación física (por hardware) entre memoria de datos y memoria de instrucciones de proceso (programa).

Las máquinas encargadas de la transferencia podrían ser las propias MGD o bien una computadora tipo PC de uso general y con seguridad local estrictamente controlada. En este último caso queda por resolver el peligro de la modificación del documento electrónico en tránsito desde la MGD a la PC.

Costo. Uno de los principales factores para la selección de la tecnología a utilizar es la inversión necesaria. En el caso de hardware de uso específico para procesos de votación, su tasa de uso temporal es extremadamente baja pero se asume que se encuentra justificada en función de la importancia y seguridad del proceso.

La inversión inicial asociada a la fabricación de un lote de pre serie seguido de un lote final en cantidades del orden de las 100.000 unidades requeridas para una votación nacional, se estima que no difiere sustancialmente del costo de adquisición de sistemas

de cómputo genéricos. A esta erogación debe sumársele el costo del depósito, traslado y custodia. No se considera la reutilización de equipamiento de voto para otros fines.

8. Consideraciones sobre el Proceso de Desarrollo de Software

Como se mencionó anteriormente, el desarrollo de un sistema de boleta única con asistencia de computadoras, en cualquiera de sus niveles de automatización de fases, constituye un sistema de misión crítica. La principal diferencia entre un sistema convencional y un sistema de misión crítica radica en la gestión del aseguramiento de la calidad, con un mayor énfasis en actividades de validación y verificación, mediante prácticas tales como: inspecciones, testing, trazabilidad, análisis de fallas, demostraciones, y aplicación de métodos formales, entre otras.

En un contexto de Ingeniería de Software, se considera que el desarrollo de software para el sistema de votación debe abordar 3 aspectos:

- El modelo de ciclo de vida (o proceso) para el desarrollo del producto.
- El ambiente en el cuál se va a desarrollar dicho producto.
- Las técnicas de desarrollo específicas que se aplicarán.

Otra premisa para dimensionar el desarrollo de software de este sistema es la realización de un análisis más detallado de su alcance, en términos de: requerimientos funcionales, requerimientos de atributos de calidad, y restricciones.

Modelo de ciclo de vida. Una práctica extendida en el desarrollo de software convencional son los modelos de ciclo de vida iterativos e incrementales, basados en Scrum, que promueven una visión ágil del proceso de construcción y una interacción fluida con el cliente (Larman, 2002). Si bien este tipo de modelos puede ser utilizado para la automatización de las últimas fases del sistema de votación, y existen experiencias aplicando métodos ágiles a sistemas de misión crítica, deben tomarse las medidas necesarias para lograr que con un método ágil se pueda lograr una gestión del aseguramiento de la calidad suficiente para el contexto del sistema. Por otro lado, no se percibe el sistema de votación como un sistema “propenso al cambio”, lo cual permitiría definir el alcance del proyecto (es decir, los requerimientos) en forma clara, para luego habilitar la aplicación de técnicas rigurosas de validación y verificación.

La idea es entonces complementar el aspecto de “agilidad” con técnicas que brinden mayor rigor y sistematicidad al proceso de desarrollo. En este sentido, *una propuesta relevante es el enfoque DAD* (*Disciplined Agile Delivery*, Ambler & Lines, 2012), que plantea un híbrido que incorpora nociones de Scrum y de arquitectura de software, y

permite también una integración del proceso base con otras técnicas (que a menudo son ignoradas por Scrum), de acuerdo a las características del proyecto. En particular, la definición de un diseño de arquitectura de software (Bass, Clements & Kazman, 2012) como parte del modelo de ciclo de vida brinda ventajas a la hora de atacar los atributos de calidad involucrados en el sistema de votación, y analizar su grado de satisfacción en la implementación. Esencialmente, una arquitectura de software puede verse como un modelo para considerar los aspectos de seguridad, confiabilidad, integridad y otros, desde fases tempranas del desarrollo.

Desde una visión tradicional para sistemas de misión crítica, se ha utilizado el denominado *modelo en V (*Scheithauer & Forsberg, 2013) que promueve actividades de validación y verificación desde etapas tempranas del proyecto. Normalmente, el modelo en V se integra sobre un ciclo de vida de cascada (*waterfall*). Básicamente, para cada actividad de la cascada se plantea una actividad asociada para validar o verificar los productos de trabajo, con distintos tipos de testing. Una problemática de esta visión es que se plantea un desarrollo de tipo secuencial. Sin embargo, existen algunas estrategias para adaptar el modelo en V a modelos de tipo iterativo-incremental, que pueden aplicarse al desarrollo del sistema de votación.

Por otro lado, se debe plantear un modelo de ciclo de vida que minimice los problemas de seguridad y otorgue sustento a los principios relacionados con la provisión de una prueba de corrección del sistema. En general, para ningún atributo de calidad, y en particular en lo que respecta a seguridad, no es recomendable incorporar mecanismos y prácticas de seguridad en las fases tardías del proceso de desarrollo. Por ejemplo, si las prácticas de seguridad se reducen a realizar un testing de seguridad al finalizar el desarrollo, es muy probable que el sistema sea esencialmente inseguro. De igual forma si las actividades de verificación se reducen a un testing de usuario o de sistema, muy probablemente el sistema contendrá un número inaceptable de errores y el proveedor no podrá aportar evidencias suficientes de la corrección del sistema. Por este motivo, el ciclo de vida debe contemplar la seguridad (y los atributos de calidad claves del sistema) desde el inicio y debe tenerla como un objetivo principal en cada fase del desarrollo. Cada decisión de diseño e implementación debe ser analizada en relación a su impacto con respecto a la seguridad y a las posibilidades de proveer una prueba de corrección del sistema. En esta línea, el equipo de desarrollo debe contar con expertos en seguridad y verificación, ya que estas tareas no pueden dejarse en manos de desarrolladores no especializados en ellas.

Ambiente de trabajo y desarrollo. Al ser un sistema de misión crítica, se deberán tener en cuenta los ambientes y prácticas que habitualmente utilizan empresas del sector para desarrollar tales sistemas. Uno de los aspectos a resaltar en este sentido es la necesidad de cumplir estándares rigurosos de desarrollo. A modo de ejemplo se mencionan algunos casos relevantes, como son:

- Los lineamientos para el desarrollo de software para sistemas de aviónica del Departamento de Defensa de EE.UU. (DO-178B) utilizado en particular por la Federal *Aviation Administration.*
- La ISO 26262 como estándar para evaluar la *safety*[8] funcional de los sistemas eléctricos o electrónicos usados en la producción de automóviles que incluyen software.
- Los estándares de la International *Electrotechnical Commission* para la producción de dispositivos médicos (IEC 62304) y para la industria nuclear (IEC 61513).
- El NASA *Software Safety Guidebook* (NASA-GB-8719.13), provee una guía para los desarrolladores de software que deben realizar análisis de *safety*. Por ejemplo, el documento discute la confiabilidad del sistema en función del *testing*: "la estimación de la confiabilidad (*reliability*) de un sistema requiere de un vasto programa de *testing*. Excepto en los raros casos donde se usan métodos formales para capturar los requerimientos y/o el diseño, el *testing* sólo puede comenzar luego de que se han generado al menos versiones preliminares del software, lo cual típicamente se da hacia el final de ciclo de vida. En ese momento, efectuar un *testing* exhaustivo está fuera del presupuesto de tiempo y recursos. En consecuencia, es difícil establecer valores precisos de confiabilidad y corrección para el software."

Se debe observar que estos estándares y guías ponen el énfasis en las propiedades de *safety* de los sistemas de misión crítica y no en las propiedades de seguridad. Si bien ambos son vocablos que informalmente significan prácticamente lo mismo, técnicamente hay una diferencia fundamental entre ambos. La mayor parte de las técnicas de Ingeniería de Software para sistemas de misión crítica apuntan a resolver el problema de *safety* y no el de seguridad. Este último requiere teorías y técnicas más complejas y menos conocidas y desarrolladas. De todas formas, existe una normativa internacional utilizada para guiar el desarrollo de sistemas de seguridad informática conocida como *Common Criteria for*

[8] Si bien "safety" se traduce como "seguridad" preferimos utilizar el término en inglés dado que "security" también se traduce como "seguridad", lo que podría dar lugar a confusiones.

Information Technology Security Evaluation (CC) o ISO/IEC 15408. El fin último de esta norma es certificar la seguridad de sistemas de cómputo. El CC fue firmado por al menos los siguientes países: Canadá, Francia, Alemania, el Reino Unido, EE.UU., Australia, Nueva Zelanda, Finlandia, Grecia, Israel, Italia, los Países Bajos, Noruega y España.

Para el desarrollo de sistemas de cómputo para el voto electrónico, en cualquiera de las fases en que se ha dividido, es altamente recomendable seguir el CC y otros estándares aplicables al desarrollo de software de misión crítica. El no hacerlo conlleva el peligro de aplicar técnicas y métodos de desarrollos obsoletos, perjudiciales y riesgosos para este tipo de sistemas.

Seguir estos estándares requiere de un grado de madurez que las empresas de desarrollo de software comercial, en general, no tienen. Por este motivo se sugiere que el proveedor demuestre idoneidad más allá del promedio de la industria (por ej., mediante la certificación de normas de calidad[9], vínculos formales con el sistema de ciencia y tecnología o el sistema universitario, etc.). En particular, el equipo técnico a cargo del proyecto debería estar integrado por profesionales con sólida formación técnica y reconocida trayectoria, incluyendo profesionales con estudios de posgrado en informática, donde algunos de ellos sean especialistas en seguridad, verificación, arquitectura de software, etc.

Respecto al *secreto del voto*, principio fundamental del sistema de votación de argentino, el desarrollo de sistemas de votación debe prestar especial atención al problema de la confidencialidad en sistemas de cómputo. En efecto, los enormes desafíos técnicos que implica intentar preservar un secreto dentro de un sistema de cómputo de propósito general, son ampliamente conocidos en la comunidad internacional de Seguridad Informática. Según la opinión de esta Comisión, no es aún un problema completamente resuelto en la práctica, aunque existen modelos teóricos que podrían garantizar tal propiedad. En particular, ninguno de los sistemas operativos comerciales de uso masivo puede garantizar esta propiedad. Por lo tanto, se desaconseja fuertemente el uso de tales sistemas en la fase de emisión del voto dado el potencial de ataque que permiten. Observar que esto implica que, de implementarse tal fase del sistema, se debería desarrollar un sistema operativo capaz de garantizar (al menos hasta donde la comunidad internacional es capaz de hacerlo) el secreto del voto.

[9] Por ejemplo, ISO, CMMI, etc.

Por otro lado, es importante resaltar que los desarrollos de software siguiendo los lineamientos y estándares antes mencionados llevan un tiempo mucho mayor al que está acostumbrada la industria de software de uso masivo, comercial o Web. Adicionalmente, debe considerarse la disponibilidad de recursos humanos calificados en el país para aplicar estas técnicas de desarrollo que, no es el caso común de las empresas de software argentinas.

Técnicas de Desarrollo. Los modelos de ciclo de vida que enfatizan aspectos de validación y verificación del software desarrollado aplican técnicas de aseguramiento de calidad que van más allá de las prácticas tradicionales de testing. Muchas de estas prácticas están tomadas del modelo en V, y están alineadas con los principios de la independencia del software y de las pruebas de correctitud del software para el fabricante/proveedor del sistema de votación.

Enfoques generalmente utilizados para dotar de mayor rigurosidad a un proceso de desarrollo de software incluyen: ingeniería conducida por modelos (MBE, por sus siglas en inglés), métodos formales para la verificación de código, *assurance cases* e inspecciones. La MBE propone la creación inicial de modelos, los cuáles se desarrollan antes de la implementación, y permiten analizar (por ej., mediante simulación) el grado de satisfacción de los requerimientos (Feiler & Gluch, 2012). Los modelos pueden incluso utilizarse para generar ciertos componentes de código o para generar casos de test. La MBE tiene un buen grado de sinergia con las prácticas de arquitectura de software. Los métodos formales constituyen una alternativa más sistemática para las técnicas tradicionales de verificación y validación (por ej., testing), ya que mediante un modelo matemático de las propiedades del sistema y de su solución (por ej., el código), pueden detectar fallas en forma automática (Brown, Delseny, Hayhurst & Wiels, 2010) y demostrar la corrección de la implementación respecto de una especificación (Boldo, Jourdan, Leroy, & Melquiond, 2015. Klein et al., 2010). El uso de técnicas formales de desarrollo ofrece tal vez, la única posibilidad de alcanzar los requerimientos sobre seguridad y corrección del software, que implemente las fases más riesgosas del proceso de votación. Debe considerarse que tanto la aplicación de MBE como de métodos formales agrega un esfuerzo importante al proceso de desarrollo y requiere personal capacitado.

Para las fases de menor riesgo, una alternativa a los métodos formales son los *assurance cases* (Rhodes, Boland, Fong & Kass, 2010), que permiten capturar evidencia sobre cierto comportamiento o propiedades del sistema, y luego mostrar (y en cierta manera,

justificar), mediante un proceso de razonamiento argumentativo, que dicho comportamiento o propiedad se cumple con un cierto grado de confianza. Estas propiedades o comportamientos pueden referirse a: seguridad, *safety*, confiabilidad, etc. Por ejemplo, se pueden construir *assurance cases* para requerimientos de seguridad, con el objetivo de mostrar que ciertas vulnerabilidades del software se han mitigado o reducido. Se destaca que el foco de los *assurance cases* está en la mitigación de los problemas o de las incertidumbres, y no en la eliminación de los mismos.

Otra técnica útil para detectar defectos son las inspecciones de software y las revisiones de pares. Estas prácticas, con distinto nivel de formalidad, se orientan a revisar un determinado artefacto de software (por ej., una especificación, un componente de software, un plan de *testing*) e identificar problemas en el mismo. Cuando estas prácticas se realizan de forma periódica en un proyecto de software, a menudo se detectan problemas (o defectos) en etapas tempranas, donde los costos de repararlas son menores, y por consiguiente se incrementa la calidad del producto.

En adherencia con el principio de desarrollo abierto, se recomienda una modalidad de desarrollo de software *open source*, que contribuya a mejorar el mantenimiento del software de votación así como la identificación (y reporte) de defectos en el mismo. La idea es que la comunidad de desarrolladores, investigadores, y ciudadanos en general puedan acceder al software y analizarlo. Si bien puede presentar ciertos desafíos en su implementación, la modalidad *open source* para sistemas de misión crítica se considera hoy una estrategia generalizada de revisión de pares que permite mejorar la calidad del sistema.

Finalmente, es conveniente remarcar como resumen que, según nuestra experiencia y por lo expuesto anteriormente, la industria del software argentina deberá realizar un esfuerzo no menor para estar a la altura (técnica) para encarar este desarrollo. Sin embargo, esto no debe verse como un impedimento sino como una oportunidad para desarrollar estas capacidades. Se considera que el país cuenta con una parte de los profesionales técnicamente capacitados para llevar adelante esta tarea y con los centros de formación e investigación para completar aspectos faltantes. Por lo tanto, creemos imprescindible poner en práctica un plan de desarrollo de alcance nacional y de mediano plazo para desarrollar o afianzar las siguientes capacidades:

- Recursos humanos competentes en aspectos de seguridad de las TICs (investigación y desarrollo).

- Recursos humanos competentes en desarrollo de software de misión crítica y altos estándares de calidad.
- Desarrollos tecnológicos de software específicos para sistemas de voto electrónico.

En relación a lo anterior, se debe tener en cuenta que la sola formación de doctores no alcanza para cubrir las necesidades a las que hacemos referencia. Se requiere un programa de formación que contemple licenciaturas o ingenierías, maestrías y, también, doctorados. Muchas de las técnicas y procedimientos necesarios para el desarrollo de este tipo de software ya son de dominio público, sólo es necesario transmitirlas a los futuros profesionales y hacer que estos estén en condiciones de aplicarlas en forma rutinaria.

9. Conclusiones y Recomendaciones

La incorporación de tecnología de software y hardware en un proceso electoral introduce *complejidades y conflictos* que no son de fácil evaluación.

Una primera conclusión de este trabajo es que debe considerarse al sistema como uno de *misión crítica*, y como tal, debe ser abordado con metodologías y técnicas específicas diferentes de las utilizadas tradicionalmente por la industria. Más aún, el desarrollo de este tipo de sistemas es de naturaleza interdisciplinaria.

Un objetivo importante en un sistema de votación es la *construcción de la confianza* que la sociedad en su conjunto va a tener sobre el sistema electoral. Debido a la importancia de los aspectos de seguridad y de construcción de confianza, se considera necesario realizar un *desarrollo abierto*, que implica que todos los artefactos (por ej., diseños, especificaciones, implementaciones, documentos de auditoría y revisiones) de todos los sistemas involucrados (hardware y software) deben estar completamente disponibles al público en general y con plazos adecuados. Esto permite que los sistemas puedan ser evaluados, con análisis forenses, progresivamente mejorados, y en última instancia se contribuya al objetivo de confianza.

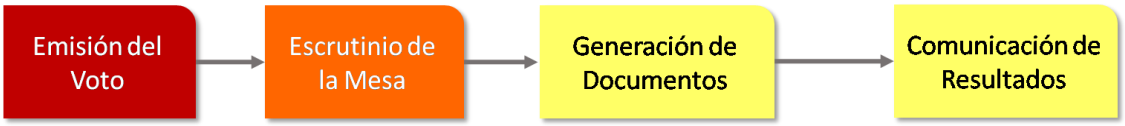
El análisis reportado en este documento asume un modelo de fases secuenciales para la votación con boleta única, donde una o más de estas fases pueden ser asistidas por computadoras.

Como se discutió a lo largo del documento es muy difícil evitar errores o vulnerabilidades en el software, por eso resulta necesario que la automatización de cada fase y la

integración de ellas resulte *independiente del software*. Esto quiere decir que el resultado de un error o cambio no detectado en el software, puede ser evidenciado por los participantes del proceso electoral.

Además, se deberá prestar especial atención a los peligros que podría introducir la integración de las distintas fases del proceso.

En el modelo de fases planteado para el dominio de la boleta única, se perciben distintos grados de riesgo y conflicto en cada una de las fases. La siguiente figura resume los niveles de riesgo identificados para cada fase según la Sección 6. Es preciso considerar que el presente informe no constituye un análisis de riesgos preciso y el mismo debería ser realizado como paso previo a cualquier solución que se decida adoptar.



Se destaca, como una segunda conclusión, que existen resultados teóricos donde se demuestra la imposibilidad de satisfacer simultáneamente tres de los atributos requeridos para el sistema (*secreto, auditabilidad e integridad*). Esto genera un compromiso entre estos atributos, que se vuelve crítico durante la fase de emisión de voto si esta fase está mediada por una computadora.

La incorporación de tecnología en las diferentes fases debe realizarse en forma gradual y progresiva, mediante proyectos piloto y a menor escala, evaluando cuidadosamente los pros y contras de cada proyecto piloto. La hoja de ruta recomendada es comenzar por las fases menos riesgosas del modelo. En particular, se recomienda no avanzar en el corto ni mediano plazo con la implementación de un sistema electrónico para la etapa de emisión de voto. En paralelo, se sugiere fomentar el desarrollo de RRHH y capacidades técnicas, e iniciar un plan de investigación que pueda aportar evidencia teórica y empírica de que los riesgos de este sistema puedan ser controlados. Los factores de complejidad y confianza antes mencionados implican esfuerzo y *programas a largo plazo*, dado que deben fortalecerse capacidades y lograrse niveles de madurez que permitan desarrollar sistemas con la calidad necesaria -- particularmente, en lo referido a aspectos de *seguridad e integridad*.

Las capacidades a desarrollar tienen que ver con:

- Recursos humanos competentes en aspectos de seguridad de las TICs (investigación y desarrollo).

- Recursos humanos competentes en desarrollo de software de misión crítica y altos estándares de calidad.
- Desarrollos tecnológicos de software SW específicos para sistemas de voto electrónico.
- Diseño de procesos operativos electorales, que combinen aspectos manuales y por computadora, planes de contingencia, etc.
- Estudios de usabilidad con sistemas piloto, que permitan evaluar los pros y contras de automatizar el sistema sobre los votantes.

Adicionalmente, es necesario garantizar procesos de evaluación, control, seguimiento y auditoría, ajustados al principio de desarrollo abierto descripto más arriba.

Por último, se desea remarcar que un proyecto de las características de un sistema de votación requiere de una entidad pública, independiente y con la capacidad técnica necesaria, que pueda ejercer la auditoría y control de los procesos y del sistema.

REFERENCIAS

Acemyan, C. Z., Kortum, P., Byrne, M. D., & Wallach, D. S. (2014). Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II. The USENIX Journal of Election Technology and Systems, 2(3), 26-56.

Agencia de Noticias del Poder Judicial. Centro de Poder Judicial Nacional (2017). La Cámara Nacional Electoral fijó pautas para la asignación de fondos públicos para la impresión de boletas. Cij.gov.ar. Recuperado el 27 septiembre de 2017, a partir de http://www.cij.gov.ar/nota-26851-La-C-mara-Nacional-Electoral-fij--pautas-para-la-asignaci-n-de-fondos-p-blicos-para-la-impresi-n-de-boletas.html

Ambler, S. W., & Lines, M. (2012). Disciplined agile delivery: A practitioner's guide to agile software delivery in the enterprise. IBM Press.

Appel, A. (2016). Which voting machines can be hacked through the Internet? Freedom to Tinker. Recuperado 15 de septiembre de 2017, a partir de https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/

Appel, A. W. (2016). Modular verification for computer security. En 29th Computer Security Foundations Symposium (pp. 1-8). Lisbon: IEEE. doi: https://doi.org/10.1109/CSF.2016.8

Aranha, D. F., Karam, M. M., de Miranda, A., & Scarel, F. B. (2014). Software vulnerabilities in the Brazilian voting machine. En Design, development, and use of secure electronic voting systems (pp. 149-175). IGI Global. doi: http://dx.doi.org/10.4018/978-1-4666-5820-2.ch008

Aris Zakinthinos, E. Stewart Lee: Composing Secure Systems that have Emergent Properties. CSFW 1998: 117-122

Axelrod, C. W. (2012). Engineering safe and secure software systems (1st ed.). Norwood: Artech House.

Axelrod, C. W. (2012). Engineering safe and secure software systems (1st ed.). Norwood: Artech House.

Babar, M. A., & Gorton, I. (2004). Comparison of Scenario-Based Software Architecture Evaluation Methods. En 11th Asia-Pacific Software Engineering Conference. IEEE. https://doi.org/10.1109/apsec.2004.38

Bannet, J., Price, D., Rudys, A., Singer, J., & Walach, D. (2004). Hack-a-vote: security issues with electronic voting systems. IEEE Security & Privacy Magazine, 2(1), 32-37. http://dx.doi.org/10.1109/msecp.2004.1264851

Bass, L., Clements, P., & Kazman, R. (2012). Software Architecture in Practice (3rd ed.). Indianapolis: Addison-Wesley Professional.

Bederson, B. B., Lee, B., Sherman, R. M., Herrnson, P. S., & Niemi, R. G. (2003, April). Electronic voting system usability issues. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 145-152). ACM.

Benaloh, J., Rivest, R., Ryan, P. Y. A., Stark, P., Teague, V., & Vora, P. (2013). End-to-end verifiablity. Recuperado de: https://www.microsoft.com/en-us/research/publication/end-end-verifiablity/

Benaloh, J., Ryan, P. Y. A., Schneider, S., & Teague, V. (2017). A Vote of Confidence? IEEE Security & Privacy, 15(3), 12-13. doi: https://doi.org/10.1109/MSP.2017.53

Boldo, S., Jourdan, J.-H., Leroy, X., & Melquiond, G. (2015). Verified compilation of floating-point computations. Journal of Automated Reasoning, 54(2), 135-163.

Brady, H. E., & Hui, I. (2008). Accuracy and security in voting systems. En Designing democratic government: making institutions work (pp. 248-297). New York: Russell Sage Foundation.

Brady, H. E., Buchler, J., Jarvis, M., & McNulty, J. (2001). Counting all the Votes. Unpublished Monograph, UC Berkeley Department of Political Science.

Brown, D., Delseny, H., Hayhurst, K., & Wiels, V. (2010). Guidance for using formal methods in a certification context. Proc. Embedded Real-time Systems and Software.

Campbell, B. A., & Byrne, M. D. (2009). Now Do Voters Notice Review Screen Anomalies? A Look at Voting System Usability. En Electronic Voting Technology Workshop/Workshop on Trustworthy Elections. Montreal: USENIX Association.

Decreto N° 2135 Texto ordenado con las modificaciones posteriores al mismo. Boletín Oficial de la República Argentina. Recuperado a partir de http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/19442/texact.htm

Drechsler, W., & Madise, Ü. (2004). Electronic voting in Estonia. Electronic Voting and Democracy. A Comparative Analysis. Basingstoke: Palgrave Macmillan, 97-108.

Everett, S. P. (2007). The usability of electronic voting machines and how votes can be changed without detection. Rice University. Recuperado a partir de http://hdl.handle.net/1911/20601

Feiler, P. H., & Gluch, D. P. (2012). Model-based engineering with AADL: an introduction to the SAE architecture analysis & design language. Addison-Wesley.

Goguen, J. A., & Meseguer, J. (1982). Security policies and security models. En Security and Privacy, 1982 IEEE Symposium on (p. 11). IEEE.

Gonggrijp, R., & Hengeveld, W.-J. (2007). Studying the Nedap/Groenendaal ES3B voting computer: A computer security perspective. En Proceedings of the USENIX workshop on accurate electronic voting technology. Berkeley: USENIX Association. Recuperado a partir de https://www.usenix.org/legacy/event/evt07/tech/full_papers/gonggrijp/gonggrijp.pdf

Gonggrijp, R., Hengeveld, W.-J., Bogk, A., Engling, D., Mehnert, H., Rieger, F., … Wels, B. (2006). Nedap/Groenendaal ES3B voting computer: a security analysis.

Hall, J. L., Stark, P. B., Miratrix, L., Briones, M., Ginnold, E., Oakley, F., … Webber, T. (2009). Implementing Risk-Limiting Post-Election Audits in California. En EVT/WOTE.

Has, F., & Ryan, P. (Eds.). (2017). Real-world Electronic Voting: Design, Analysis, and Deployment. Boca Raton: Taylor and Francis.

High-Assurance Systems | SRI International. (2017). Retrieved September 15, 2017, from https://www.sri.com/research-development/high-assurance-systems

Hosp, B., & Vora, P. L. (2008). An information-theoretic model of voting systems. Mathematical and Computer Modelling, 48(9-10), 1628-1645. doi: https://doi.org/10.1016/j.mcm.2008.05.040

Jacobs, B., & Pieters, W. (2009). Electronic Voting in the Netherlands: from early Adoption to early Abolishment. En Foundations of security analysis and design V (pp. 121-144). Berlin Heidelberg: Springer. doi: https://doi.org/10.1007/978-3-642-03829-7_4

Kerckhoffs, A. (1883). La cryptographie militaire La cryptographie militaire, ou, Des chiffres usités en temps de guerre: avec un nouveau procédé de déchiffrement applicable aux systèmes à double clef. Journal des sciences militaires, IX, 5-38.

Kimball, D. C., Owens, C., & McAndrew, K. (2002). Unrecorded votes in the 2000 presidential election. Similar to a paper later published at APSA99.

Klein, G., Norrish, M., Sewell, T., Tuch, H., Winwood, S., Andronick, J., … Kolanski, R. (2010). seL4. Communications of the ACM, 53(6), 107. https://doi.org/10.1145/1743546.1743574

Klein, G., Norrish, M., Sewell, T., Tuch, H., Winwood, S., Elphinstone, K., … Kolanski, R. (2009). seL4. En Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles - SOSP '09. ACM Press. https://doi.org/10.1145/1629575.1629596

Kulyk, O., Neumann, S., Budurushi, J., & Volkamer, M. (2017). Nothing Comes for Free: How Much Usability Can You Sacrifice for Security? IEEE Security & Privacy. https://doi.org/10.1109/MSP.2017.70

Lampson, B. W. (1973). A note on the confinement problem. Communications of the ACM, 16(10), 613-615. Recuperado a partir de https://cacm.acm.org/magazines/1973/10/11817-a-note-on-the-confinement-problem/abstract

Larman, C. (2004). Agile and iterative development: a manager's guide. Addison-Wesley Professional.

Loeber, L. (2008). E-voting in the Netherlands; from general acceptance to general doubt in two years. En 3rd international Conference on Electronic Voting (Vol. 131, pp. 21-30). Bregenz: Gesellschaft für Informatik.

Mantel, H. (2002). On the composition of secure systems. En IEEE Symposium on Security and Privacy (pp. 88-101). Berkeley: IEEE. doi: https://doi.org/10.1109/SECPRI.2002.1004364

Mantel, H., Sands, D., & Sudbrock, H. (2011). Assumptions and guarantees for compositional noninterference. En 24th Computer Security Foundations Symposium (pp. 218-232). Cernay-la-Ville: IEEE. doi: https://doi.org/10.1109/CSF.2011.22

Mercuri, R. (2017). Electronic Voting. Notablesoftware.com. Recuperado el 27 septiembre de 2017, a partir de: http://www.notablesoftware.com/evote.html

Mercuri, R. T. (2001). Electronic vote tabulation checks and balances. Dissertations available from ProQuest. Recuperado a partir de http://repository.upenn.edu/dissertations/AAI3003665

Montes, M., Penazzi, D., & Wolovick, N. (2016). Consideraciones sobre el voto electrónico. En 10° Simposio de Informática en el Estado - 45° Jornadas Argentinas de Informática (pp. 297-307). Tres de Febrero: Sociedad Argentina de Informática e Investigación Operativa. Recuperado a partir de http://45jaiio.sadio.org.ar/sites/default/files/SIE-27.PDF

National Democratic Institute. (2017). The Constitutionality of Electronic Voting in Germany. Recuperado 15 de septiembre de 2017, a partir de https://www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany

Norris, J. S. (2004). Mission-critical development with open source software: Lessons learned. IEEE Software, 21(1), 42-49. doi: https://doi.org/10.1109/MS.2004.1259211

Oren, Y., & Wool, A. (2010). RFID-based electronic voting: What could possibly go wrong? En International Conference on RFID (pp. 118-125). Orlando: IEEE. doi: https://doi.org/10.1109/RFID.2010.5467269

Press Release. Independent Report on E- voting in Estonia. (12 de mayo de 2014). Recuperado a partir de: https://estoniaevoting.org/press-release/

Rhodes, T., Boland, F., Fong, E., & Kass, M. (2010). Software assurance using structured assurance case models. Journal of research of the National Institute of Standards and Technology, 115(3), 209.

Rivest, R. L. (2008). On the notion of «software independence» in voting systems. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 366(1881), 3759 LP - 3767. doi: http://dx.doi.org/10.1098/rsta.2008.0149

RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," December 1, 1992.

RTCA/DO-178C Software Considerations in Airborne Systems and Equipment Certification. RTCA, Inc. 2011.

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. Proceedings of the IEEE, 63(9), 1278–1308. doi: https://doi.org/10.1109/PROC.1975.9939

Scarfone, K. A., Jansen, W., & Tracy, M. (2008). Guide to general server security. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-123

Scheithauer, D., & Forsberg, K. (2013). 4.5.3 V-Model Views. En INCOSE International Symposium (Vol. 23, pp. 502-516). Philadelphia: Wiley. doi: http://dx.doi.org/10.1002/j.2334-5837.2013.tb03035.x

Sutherland, I., Korelsky, T., McCullough, D., Rosenthal, D., Seldin, J., Lam, M., … Perlo, S. (1991). Romulus: A Computer Security Properties Modeling Environment. Nueva York. Recuperado a partir de http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA236129

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency Planning Guide for Federal Information Systems. NIST Special Publication 800-34 Rev. 1. Gaithersburg: U. S. Department of Commerce. National Institute of Standards. Recuperado a partir de http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Technical Guidelines Development Committee. (2007). Voluntary voting system guidelines recommendations to the election assistance commission. Election Assistance Commission, Washington DC, USA.

U.S. Election Assistance Commission. (2017). Starting Point: U.S. Election Systems as Critical Infrastructure. Silver Spring. Retrieved from https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf

Voightmann, M. P., & Coleman, C. P. (2003, May). Open source methodologies and mission critical software development. In 3rd. Workshop on Open Source Software Engineering (p. 137).

Voting System Reports Collection - Voting Equipment | US Election Assistance Commission. (2017). Eac.gov. Retrieved 27 September 2017, from https://www.eac.gov/voting-equipment/voting-system-reports-collection/

Winckler, M., Bernhaupt, R., Palanque, P., Lundin, D., Leach, K., Ryan, P., ... & Strigini, L. (2009). Assessing the usability of open verifiable e-voting systems: a trial with the system Prêt à Voter. Proc. of ICE-GOV, 281-296.

ANEXO: ESCENARIOS DE CALIDAD

La tabla asociado en el presente anexo tiene una finalidad demostrativa de la evaluación metodológica propuesta. El listado de escenarios no es un análisis exhaustivo y de ninguna manera son las bases para concluir sobre una realización particular de un sistema de votación electrónica.

Nro.	Atributo(s) de Calidad	Descripción del Escenario	Fases (a las que aplica cada escenario)			
			Comunicación de Resultados	Generación de Documentos	Escrutinio de Mesa	Emisión de Votos
1	seguridad/ confiabilidad/ performance	El sistema de cómputo (impresora/computadora) genera documentación en papel incorrecta.		X		
2	usabilidad/ confiabilidad/ performance	El sistema de impresión se corrompe y no se puede utilizar.		X		
3	seguridad/ integridad/ performance	El sistema imprime copias que son distintas (variante del 1)		X		
4	seguridad/ integridad/ performance	El contenido digital del documento no coincide con el impreso		X		
5	seguridad	Los documentos electrónicos son alterados en tránsito.	X			
6	usabilidad/ confiabilidad	No es posible enviar los documentos electrónicos.	X			
7	seguridad/ integridad/ performance	El conteo electrónico de los votos no coincide con las boletas en papel.			X	

Nro.	Atributo(s) de Calidad	Descripción del Escenario	Fases (a las que aplica cada escenario)			
			Comunicación de Resultados	Generación de Documentos	Escrutinio de Mesa	Emisión de Votos
8	seguridad/ integridad	El sistema de conteo no garantiza el anonimato de los votantes.			X	X
9	seguridad	Es posible asociar votos a votantes.				X
10	seguridad/*fairness* (garantizar la oferta política)	La máquina emisora de boletas favorece o perjudica a uno o más candidatos en forma oculta.				X
11	seguridad/ usabilidad	El sistema genera boletas distintas a la selección del votante.				X
12	usabilidad/ confiabilidad	La máquina emisora de boletas se daña y no puede brindar servicio.				X
13	usabilidad	La máquina emisora de boletas no es simple/intuitiva de usar por los votantes.				X
14	seguridad	La máquina emisora de boletas es manipulada para cambiar su comportamiento o dañarla irreversiblemente.				X
15	performance	Luego de terminada una elección, se realiza el conteo de los votos de manera eficiente (volumen, throughput) y con una baja tasa de errores	X	X	X	

Nro.	Atributo(s) de Calidad	Descripción del Escenario	Fases (a las que aplica cada escenario)			
			Comunicación de Resultados	Generación de Documentos	Escrutinio de Mesa	Emisión de Votos
16	auditabilidad/ confiabilidad	Ante un problema en el conteo en una mesa, es posible chequear los votos (electrónicos) del sistema contra los votos en papel, y detectar las diferencias		X	X	
17	SW *independence* (*testability*)	Se realiza un proceso de testing del SW del sistema, con una cobertura X, en un tiempo Y, a fin de aproximar la detección de fallas en SW.		X	X	X
18	confiabilidad	Ante una falla en un scanner óptico, es igualmente posible almacenar el voto para un futuro conteo automatizado (asistido)			X	
19	usabilidad/fairness	Dado un gran número de candidatos a ser elegidos, el sistema presenta al usuario la lista de candidatos en un orden o disposición que no perjudique a ningún candidato, y que a la vez evite la "sobrecarga de información" para el votante				X
20	seguridad	El software del sistema de emisión no coincide con el auditado		X	X	X

CONSEJO NACIONAL DE
INVESTIGACIONES CIENTÍFICAS Y TÉCNICAS
Godoy Cruz 2320, Buenos Aires - 011 4899-5000