

Identification of Non-Functional Requirements for Electronic Voting Systems: A Systematic Mapping

S. Sepúlveda, *Member, IEEE*, M. Bustamante, and A. Cravero

Abstract— **Background:** Given the level of technological progress made today is that civic and government institutions seek to replicate the success of systems like the financial sector and banking in electronic voting systems. **Objective:** To make an analysis for the developed systems to conduct electronic voting from the Requirements Engineering perspective. **Method:** We use the methodology of systematic mapping study. **Initially,** we collect 240 publications and finally selecting 60 works. The Non Functional Requirements selected were Security, Performance efficiency, Reliability and Operability, which were chosen from several publications suggesting that this group was critical to the successful adoption of electronic voting systems. **Results:** The results show that 49% of the proposals considered Security feature the most relevant, which is consistent with the literature. The 23% of publications addressing Performance Efficiency, revealing that the main problem today is to build a model of electronic voting that is safe and can be widely implemented dedicating a reasonable amount of resources. **Conclusions:** A set of recommendations was generated. Given the complexity of evote systems, these must be addressed holistically.

Keywords— Non Functional Requirements, electronic voting, systematic mapping study

I. INTRODUCCIÓN

ACTUALMENTE, la democracia es la forma de gobierno imperante en el mundo occidental y constituye un pilar fundamental en la construcción de la sociedad. Tradicionalmente las elecciones han sido efectuadas en formato manual por parte de los electores usando lápiz y papel, pero dado el avance tecnológico experimentado durante los últimos 50 años se ha propuesto introducir elementos electrónicos a las votaciones a fin de mejorar el proceso eleccionario. Un ejemplo de adopción de sistemas electrónicos dentro de un Estado, es el caso del Servicio de Impuestos Internos de Chile, el que permite observar cómo se puede disminuir la burocracia y al mismo tiempo aumentar la cobertura de servicios utilizando medios electrónicos.

La pregunta entonces es, si es posible extender el uso de esos sistemas electrónicos a las votaciones electorales que definen nuestros gobernantes. La votación electrónica (e-voting), se refiere generalmente a diferentes tipos de votación que utilizan medios electrónicos para emitir el voto y/o para su conteo. Estos métodos aún no están consolidados como alternativa a las votaciones tradicionales, ya que existen dudas de que estos sistemas sean capaces de garantizar derechos

constitucionales y al mismo tiempo evitar fraudes electorales o sabotajes.

Experiencias reales de votación electrónica hay varias y con diversos resultados. A lo largo del tiempo se han utilizado varios Sistemas de Votación Electrónica (SVE) en países como: Brasil, India, Estados Unidos, Estonia, Francia, Venezuela, Holanda, Reino Unido, Suiza y Canadá. Estos han sido usados en distintas tipos de votaciones: elecciones presidenciales, senatoriales, municipales y referéndums.

Desde el 2000 los avances sobre la construcción de SVE más seguros y confiables se han intensificado de acuerdo a las decisiones políticas tomadas por los gobiernos de E.E.U.U. y la Unión Europea, pero el consenso en la comunidad es que si bien la votación electrónica permite mejorar las votaciones tradicionales, aún tiene problemas pendientes a solucionar. Aparte de las consideraciones técnicas, un SVE es “tan bueno como el pueblo piensa que es”, en este sentido los sistemas deben ser capaces de demostrar que son confiables, no sólo a nivel de seguridad sino también de usabilidad y accesibilidad.

El problema es entonces, cómo poder garantizar a la población de que los SVE son buenos en el amplio sentido de la palabra. Siendo el software una parte muy importante de éstos sistemas, debemos ser capaces no sólo de construir software que permita a las naciones elegir sus gobernantes de forma rápida y eficiente, sino también de poder medir su calidad de forma objetiva para poder construir sistemas legítimos para el pueblo.

Este trabajo busca abordar el problema de la calidad del software de los SVE analizando los aspectos que más se han trabajado en este tema, dentro del marco del estándar de calidad ISO 25010:2011. A partir de esos resultados se desea establecer un conjunto de recomendaciones que permitan profundizar en la noción de calidad en futuros modelos y SVE. La idea fundamental consiste en identificar y evaluar los Requerimientos No Funcionales (RNF) presentes en modelos y SVE, usando para esto la metodología de mapeo sistemático.

El mapeo sistemático, según [1], es un método robusto y repetible usado particularmente para responder de forma metódica, objetiva y libre de sesgo un conjunto de preguntas de investigación, identificando los principales estudios que pueden contener información relevante (búsqueda), seleccionando los estudios pertinentes después de mayor revisión (inclusión/exclusión) y donde es apropiado, realizar una evaluación de calidad de los estudios seleccionado (sesgo/validez). Para efectos de este trabajo se ha seguido el protocolo para la conducción de mapeos sistemáticos en el dominio de la Ingeniería de Software (IS) definido por [2].

El resto de este artículo se estructura como sigue. Sección II presenta una breve descripción de conceptos previos. La Sección III describe el proceso de mapeo sistemático

S. Sepúlveda, Universidad de La Frontera, Chile, samuel.sepulveda@ceisufo.cl

M. Bustamante, Universidad de La Frontera, Chile, m.bustamante01@ufromail.cl

A. Cravero Universidad de La Frontera, Chile, ania.cravero@ufrontera.cl

realizado. En la Sección IV se presentan y discuten los resultados del trabajo, así como un conjunto de recomendaciones para el desarrollo de SVE. Finalmente la Sección V presenta las conclusiones y trabajos futuros para el estudio realizado.

II. CONCEPTOS PREVIOS

En esta sección presentamos un conjunto de trabajos que resumen la evidencia en el área de SVE (ver Sección A), la Ingeniería de Requerimientos (ver Sección B) y al estándar ISO 25010 (ver Sección C).

A. *Sistemas de Votación electrónica (SVE)*

En el marco de este trabajo un SVE se entiende como el sistema donde el registro, interpretación o conteo de los votos en elecciones y referendums políticos involucra tecnologías de información y comunicación [3]. Por su parte la Unión Europea ha definido un conjunto de derechos y deberes para sus estados miembros con respecto a las elecciones [4]. Además, la comisión de Venecia del Consejo Europeo, generó un código de buenas prácticas en materia electoral [5]. Si bien los conceptos y términos que son utilizados en este dominio son bastante amplios, existe consenso en algunos conceptos básicos como los que plantean [6], [7].

Los procesos electorarios, además de diferenciarse según las regulaciones legales de cada país, se diferencian según la forma de cómo se llevan a cabo. En cuanto a la votación electrónica, se tienen dos variantes: en estación y a través de Internet [8]. De igual forma éstas pueden clasificarse dependiendo del tipo de tecnología que utilizan: (i) Máquinas DRE, (ii) Sistemas OMR, (iii) Impresoras de papeletas electrónicas y (iv) Sistemas de voto por internet [3].

Este conjunto de obligaciones conforman una serie de requisitos que los SVE deben satisfacer. Es por esto que resulta crítico garantizar el correcto funcionamiento de los SVE, abordando las amenazas y estableciendo mecanismos que garanticen la integridad del proceso electoral [9].

B. *Ingeniería de Requerimientos*

La Ingeniería de requerimientos (IR) se refiere al proceso de formular, documentar y mantener requerimientos de software [10]. El SWEBOK V3 se refiere a ésta como el proceso que aborda la educación, análisis, especificación y validación de requerimientos de software como también la gestión de requerimientos durante todo el ciclo de vida del software [11]. Básicamente, un requerimiento de software es una propiedad que debe ser exhibida por el software en algún nivel para poder resolver un problema. Los requerimientos son clasificados principalmente en dos tipos: funcionales y no funcionales.

La definición del término RNF no está absolutamente consensuada, pues podemos encontrarnos con diversos autores y sus propias definiciones ([10], [12], [13]). Sí existe un consenso en que todas las definiciones de RNF se basan en los términos propiedad o característica, atributo, calidad, restricción y rendimiento aún cuando no existe un consenso en cuánto a los conceptos que éstos términos denotan [14].

Finalmente podemos decir que los RNF son aquellos que actúan para restringir la solución y pueden ser clasificados de acuerdo a las características de modelos de calidad, como requerimientos de rendimiento, confiabilidad, interoperabilidad o seguridad, entre otros [11].

C. *Estándar ISO/IEC 25010*

El estándar ISO/IEC 25010:2011 [15] es una revisión del estándar 9126-1:2001[16], que incorpora similares características de calidad de software y un modelo de calidad de producto. Las 8 características son divididas en subcaracterísticas, que se refieren a propiedades estáticas de software y propiedades dinámicas de sistemas de computación.

Las características y subcaracterísticas proveen de una terminología consistente para la calidad de producto de software. También proveen un conjunto de características de calidad las cuales pueden ser comparados con requerimientos de calidad. Los modelos de calidad pueden ser usados para asistir la especificación y evaluación de software desde distintas perspectivas relacionadas con la adquisición, requerimientos, desarrollo, uso, evaluación, soporte, mantenimiento, aseguramiento de la calidad y auditorías de software.

Dada la extensión del estándar ISO/IEC 25010:2011, sólo se describirán las subcaracterísticas que interesan a los SVE de acuerdo a lo desprendido por distintos autores y que luego serán utilizados para la construcción del mapeo sistemático. Los argumentos para justificar la elección de las 4 características: Security, Reliability, Performance efficiency y Operability pueden revisarse en [17] - [20]. En este trabajo se considera que las características y subcaracterísticas planteadas en el ISO/IEC 25010 están relacionadas con RNF ya que se basan en atributos de calidad que los SVE pueden satisfacer.

III. PROCESO DEL MAPEO SISTEMÁTICO

De acuerdo a la metodología de mapeo sistemático planteada por [2], se llevaron a cabo las etapas que ésta contempla.

Primero se establecieron los lineamientos generales del trabajo que fueron definidos por uno de los investigadores y validados por un segundo investigador (ver Sección A). Luego, se definieron las preguntas de investigación (PI), las que plantean lo que el trabajo debe responder (ver Sección B). A continuación, se definieron la cadena de búsqueda, las fuentes de datos y los criterios de inclusión y exclusión (ver Sección C). La siguiente etapa consistió en buscar las publicaciones y extraer los datos necesarios para su documentación (ver Sección D). Luego, se procedió a clasificar los trabajos utilizando *keywording* para la posterior aplicación de los criterios de inclusión y exclusión, obteniendo así un conjunto final de trabajos seleccionados (ver Sección E). Obtenido este conjunto de publicaciones (ver Sección F), se procedió a clasificar las publicaciones según varios ejes de clasificación (ver Sección G). Finalmente se procedió con la extracción de datos y construcción del mapa (ver Sección H).

A. *Lineamientos generales del problema*

La necesidad de la investigación radica en que el consolidar los SVE ayudaría a resolver uno de los mayores problemas de la democracia directa: la dificultad física de distribuir información a una gran población, generar debate y recolectar sus votos. Los SVE están lejos de estar consolidados, por lo que existe una gran diversidad de criterios sobre qué modelos se deberían construir y cómo se

deberían implementar.

La idea de utilizar la metodología de mapeo sistemático se justifica puesto que necesitamos obtener un conjunto relevante de trabajos relacionados con los SVE para identificar y evaluar los RNF presentes y generar así un conjunto de recomendaciones.

B. Preguntas de investigación

Las PI se plantean a partir de los objetivos del trabajo y la motivación que existe para aplicar el mapeo sistemático. Las PI definidas son:

- PI-1: De los estudios seleccionados ¿Cuántos plantean modelos (o propuestas teóricas)? ¿Cuántos plantean implementaciones de SVE?
- PI-2: Para los modelos o implementaciones de SVE ¿Cuántos estudios abordan los RNF?
- PI-3: ¿Cuáles son los RNF abordados por los estudios acorde a lo definido en la norma ISO/IEC 25010?

C. Conceptos clave y cadenas de búsqueda

Para construir la cadena de búsqueda se extrajeron desde las PI y los objetivos del trabajo un conjunto de palabras clave. Dichas palabras clave se concatenaron usando conectores lógicos. Esta cadena de búsqueda fue probada iterativamente en los motores de búsqueda y validada entre los investigadores. Al realizar la búsqueda, dicha cadena se aplicó sólo al abstract de los trabajos, puesto que una búsqueda en todo el texto de los trabajos resultaba en un conjunto demasiado amplio para el análisis. Se estableció además que las palabras clave no incluyesen ninguna relación con RNF, puesto que las pruebas preliminares arrojaron un conjunto de publicaciones muy pequeño e incluso a veces vacío. La cadena resultante fue: ('electronic voting' OR e-vote) AND (model OR scheme OR proposal OR protocol OR system).

D. Búsqueda y extracción de datos

Se consideraron fuentes que contaran con sitios web donde se pudiera acceder a bibliotecas digitales con motores de búsqueda implementados. Lo anterior considera entonces elegir fuentes con una gran cantidad de artículos relativos a las ciencias de la computación y que brinden la capacidad de buscar trabajos usando cadenas de búsqueda y operadores lógicos. Las fuentes de datos seleccionadas: IEEE Xplore, ACM Digital Library y Science Direct, reconocidas entre las más reputadas dentro de la comunidad de IS [21].

E. Criterios de inclusión y exclusión

Sólo se consideraron artículos de revistas científicas y actas de congresos, esto con el fin de acceder a propuestas maduras o que mostraran experiencia de implementaciones de SVE. Se excluyeron entre otros, libros, sitios web y reportes técnicos.

A continuación se listan los criterios considerados.

- Criterios de inclusión
 - Estudios que propongan modelos de votación electrónica
 - Estudios que aborden RNF en SVE
 - Estudios que aborden SVE existentes
- Criterios de exclusión
 - Estudios que se enfoquen en votaciones distintas a las electorales
 - Estudios enfocados en votaciones de pequeño alcance

- Estudios criptográficos en que su aplicación principal no sea la votación electrónica
- Estudios que no aporten mejoras significativas a propuestas anteriores

F. Ejecución de la búsqueda

Se aplicó la cadena de búsqueda en las fuentes seleccionadas y se obtuvo una cantidad inicial de 321 trabajos, la información fue extraída usando las herramientas de exportación de cada una de las bibliotecas digitales. Tras eliminar aquellos trabajos que se encontraban doblemente indexados, se redujo a 240 trabajos. Luego, se aplicó el criterio de inclusión/exclusión, quedando 101 trabajos. A continuación, se comenzó con la etapa de *keywording*, la cual se realizó leyendo los abstracts, palabras clave e introducción de cada trabajo y etiquetándolos según correspondiera. Se iteró dos veces esta etapa para verificar que el criterio de etiquetado fuese uniforme. Finalmente se hizo una lectura más detallada de cada trabajo para evaluar su pertinencia al mapeo, obteniendo un total de 60 trabajos.

G. Esquema de clasificación

Las publicaciones son clasificadas en 3 dimensiones: temporal, subcaracterísticas de calidad y tipo de propuesta. La dimensión temporal clasifica los trabajos de acuerdo al año de publicación, tomando en cuenta los últimos 10 años, período 2003-2013.

La dimensión subcaracterísticas de calidad clasifica los trabajos de acuerdo a cual de las subcaracterísticas se enfoca el estudio, según el estándar ISO/IEC 25010:2011. Si bien hay trabajos que pueden ser clasificados en más de una subcaracterística, se construyeron categorías a partir de la combinación de las subcaracterísticas, tal cual se ha visto en trabajos similares [22].

La dimensión tipo de propuesta clasifica los trabajos en:

- Solución criptográfica: plantean soluciones problemas detectados en otros modelos centrados en criptografía (auditorías a otros modelos, detección de errores y propuestas de mejora).
- Propuesta criptográfica: plantean o mejoran métodos criptográficos para una o varias funciones de los SVE (modelos que satisfagan requisitos básicos de la votación electrónica mediante la construcción de protocolos o esquemas criptográficos).
- Modelo: plantean modelos generales de SVE (uso de métodos criptográficos, revisiones/comparaciones con otros modelos, o que aborde otras funciones dentro del proceso electoral).
- Implementación: además de plantear un modelo, describen temas asociados a su implementación (su construcción total/parcial o experiencias de su puesta en marcha).

H. Mapeo sistemático

El producto final del mapeo sistemático fue dividido en 2 mapas para facilitar su representación y análisis. La Fig. 1 muestra todos los estudios que fueron clasificados en sólo una categoría. La Fig. 2 muestra aquellos que fueron clasificados en múltiples categorías. Revisando ambas figuras, se desprende que los trabajos mayoritariamente plantean modelos y sólo una pequeña parte presenta implementaciones de SVE.

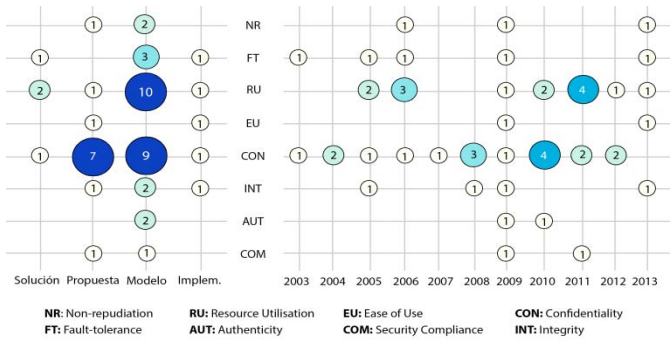


Figura 1. Mapa de subcaracterísticas de ISO/IEC 25010 en modelos e implementaciones de SVE

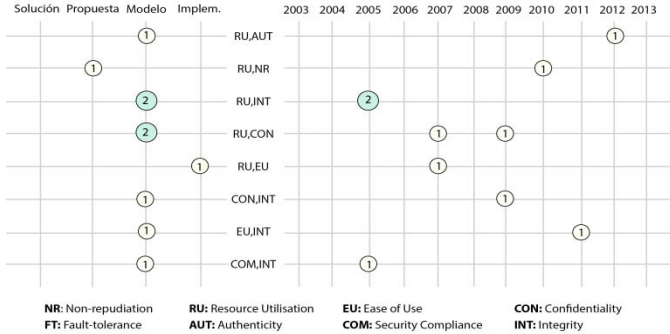


Figura 2. Mapa de múltiples subcaracterísticas de ISO/IEC 25010 en modelos e implementaciones de SVE

En la Fig. 2 se observa la baja cantidad de trabajos que explícitamente abordan más de un RNF. Se observa además que la subcaracterística que más se conjuga con otras es Resource Utilisation, seguido por Integrity, lo cual es consistente con lo dicho anteriormente, que son los aspectos inherentes de los protocolos criptográficos los que se ven reflejados en los RNF.

IV. ANÁLISIS DE RESULTADOS Y DISCUSIÓN

Dada la cantidad de modelos y sistemas propuestos en la literatura, está claro que la votación electrónica es un área con bastante actividad científica. A continuación se presentan las respuestas a las PI (ver Sección A), luego damos cuenta de un conjunto de hallazgos y recomendaciones (ver Sección B), finalmente se presentan las amenazas a la validez de trabajo propuesto (ver Sección C).

A. Respondiendo a las preguntas de Investigación

PI-1: De los estudios seleccionados ¿Cuántos plantean modelos (o propuestas teóricas)? ¿Cuántos plantean implementaciones de SVE?: Se identificaron 60 trabajos, publicados entre 2003 y 2013, que planteaban algún modelo, propuesta o implementación de un SVE. De estos, 55 trabajos presentaban a nivel teórico y sólo 5 trabajos presentaban implementaciones de SVE.

PI-2: Para los modelos o implementaciones de SVE ¿Cuántos estudios abordan los RNF?: Dada la búsqueda y selección de trabajos realizada, resultó finalmente que los 60 trabajos seleccionados al menos mencionan un RNF enmarcado dentro de las subcaracterísticas presentadas en el estándar ISO/IEC 25010. La clasificación y detalle puede verse en las Fig. 1 y 2.

PI-3: ¿Cuáles son los RNF abordados por los estudios acorde a lo definido en la norma ISO/IEC 25010?: De los

RNF revisados en los estudios seleccionados, fueron encontrados sólo 8. Con 18 trabajos (30%) aparece Confidentiality, luego Resource Utilisation con 14 trabajos (23%), 5 trabajos (8%) para Fault Tolerance, con 4 y 3 trabajos (6% y 5 %) respectivamente aparecen Integrity y Non-Repudiation, finalmente con 2 trabajos cada uno (3%) aparecen Ease of Use, Authenticity y Security Compliance. Se deben considerar además 10 trabajos (16%) que consideran una combinación de 2 RNF. Estos resultados son consistentes con la literatura analizada en capítulos anteriores ya que se observa una presencia predominante de aspectos asociados a protocolos criptográficos: seguridad y recursos computacionales necesarios para ejecutarlos.

B. Hallazgos y recomendaciones

• Seguridad y otros aspectos de Calidad

Se observa que los esfuerzos están puestos en formular e implementar algoritmos y modelos de seguridad comprobada, con 29 trabajos (49%). Si bien se entiende que para los SVE la seguridad es crítica, ¿Por qué existen tan pocos trabajos en otros aspectos de calidad? Por ejemplo sólo 5 trabajos (8%) se enfocan Reliability y apenas 2 trabajos (3%) se enfoca en temas Operability. Una posible explicación de la actual situación de los SVE es que simplemente no es posible hacerlo de forma [7]. Luego podemos afirmar que si aún no se resuelven los temas de seguridad, difícilmente se puede enfocar en otros aspectos de calidad de software.

Los estudios revisados además indican que en general la aplicación de modelos de calidad a la propuesta e implementación de SVE es un área inmadura. Se puede ver que 37 trabajos (61%) corresponden a modelos teóricos. Hay 13 trabajos (22%) que se enfocan en propuestas criptográficas. Sólo 6 trabajos (10%) reportan uso, implementación y/o evaluación de características de calidad. Una posible explicación de este fenómeno es que los SVE suelen ser de código cerrado, y sólo algunas personas tienen acceso a información detallada acerca de cómo funcionan. De acuerdo con lo planteado por [23], faltan esfuerzos en construir programas de código abierto, simplificar la implementación de estos sistemas y mejorar la transparencia, para poder conseguir que la votación electrónica sea una aplicación exitosa de tecnología. Finalmente, 4 trabajos (7%) presentan soluciones criptográficas.

La eficiencia es un aspecto que varios estudios toman en cuenta, pero con distintos puntos de vista puesto que algunos lo utilizan para hacer su protocolo/esquema práctico, en el sentido de que es posible usarlo en votaciones reales mientras que otros se enfocan explícitamente en votaciones a gran escala. Entonces, aparece el problema de proveer una solución que satisfaga la definición de seguridad más fuerte o encontrar protocolos eficientes que puedan ser implementados a gran escala.

• Requerimientos y restricciones para los SVE

Usualmente cada propuesta de SVE define su propio conjunto de requisitos a satisfacer, los cuales no se deben asociar directamente con requerimientos de software, puesto que los primeros no necesariamente involucran software. Varios estudios han definido informalmente una lista de requerimientos para los SVE, [24] propone 8 requisitos fundamentales a considerar: privacy, eligibility, uniqueness, fairness, uncoercibility, receipt-freeness, accuracy e individual

verifiability. Pese a esto, existen ligeras diferencias al definir los requisitos entre distintos estudios, y varias de estas definiciones son incompatibles con otros modelos de votación electrónica [25]. Las propuestas de [6], [26] contienen los requisitos que más aceptación concitan en la literatura.

La idea de definir dichos requisitos es establecer un marco de trabajo dentro del cual debe regirse la implementación de un SVE, dado a que actualmente no existen estándares y requisitos globalmente aceptados. Así entonces, cada país debe definir estos requisitos basado en los acuerdos legales locales e internacionales, para poder ser implementados y adoptados en procesos eleccionarios [3]. No todos los requisitos anteriormente expuestos pueden ser satisfechos al mismo tiempo, y como indica [27], las propuestas suelen enfocarse en satisfacer un subconjunto de todos los requerimientos expuestos y balancean su cumplimiento para lograr SVE que puedan poner en práctica.

- Enfoques para diseño de los SVE

Si bien existe un marco legal aceptado internacionalmente sobre el proceso eleccionario, existen diferencias al traducirlo a un conjunto de requisitos que los SVE deben satisfacer. A partir de un modelo general del proceso eleccionario, [28] propone un modelo de SVE genérico usando Diagramas de Casos de Uso UML, donde se definen los principales actores y funcionalidades de estos sistemas. Otro enfoque que permite comprender los SVE es el ortogonal, que propone dividir los SVE en 4 capas: humana, de elección, computacional y física. Cada capa está constituida por un conjunto de componentes. La ventaja de este enfoque es que cada componente puede tener su propio análisis de amenazas, disminuyendo los riesgos del sistema completo al hacer cambios focalizados [29]. Luego, se puede proponer una primera aproximación de los SVE y del cómo estos pueden asociarse con RNF basados en un modelo de calidad de software. Por ejemplo la capa humana se relaciona con la característica Operability, pues ambas se refieren a la interacción entre los recursos humanos y el sistema electrónico.

- Jerarquización de características de Calidad

Dados los resultados del estudio, se propone una jerarquización dentro de las 8 características del modelo de calidad ISO/IEC 25010. La Fig. 3 muestra las 8 características, siendo la prioridad máxima Security, en segundo lugar Reliability, Operability y Performance Efficiency, para dejar en tercer lugar Maintainability, Portability, Functional Suitability y Compatibility. El objetivo que tiene esta jerarquización es la de orientar la construcción y evaluación de SVE que generen confianza. La seguridad por sí sola no lo asegura, puesto que como plantea [20], algunas suposiciones de seguridad hacen impracticables los protocolos en elecciones de gran tamaño.

- Construir y mantener SVE usando software de código abierto

El utilizar código abierto tiene 2 finalidades: transparencia y seguridad. Actualmente los SVE son de código cerrado, es decir, usualmente sólo personas que pertenecen a la organización encargada de mantener el software tienen acceso al código fuente y a la tecnología utilizada. Actualmente varias naciones licitan máquinas y software a sólo una empresa, por lo que es posible que queden amarradas (*vendor lock-in*) a la tecnología que dicha empresa distribuya. Usando código abierto sería posible disminuir la dependencia a una

sola entidad puesto que es posible integrar tecnologías de distintos proveedores [27].

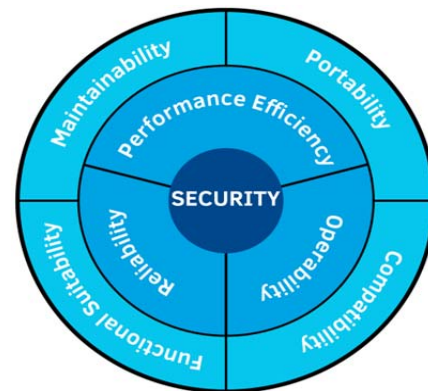


Figura 3. Jerarquización de las características ISO/IEC 25010 en modelos de votación electrónica

- Uso de enfoques Holísticos

Al ser la votación una manifestación socio-política, la adopción de los SVE debe considerar el factor humano, incluyendo no sólo aspectos de seguridad, sino otras características presentes en los modelos de calidad de software como: Reliability, Usability, Maintainability y Portability. Incluso en países con casos de éxito, problemas de seguridad relativos a la administración revelan el nivel actual de los SVE y su potencial adopción por otras naciones [18]. Al ampliar la mirada a todos los componentes de un SVE aparecen problemas como la imposibilidad de garantizar que todos los ciudadanos, incluyendo discapacitados o ancianos, sean capaces de votar en sistemas de votación puramente electrónicos. Es por esto que se recomienda al plantear modelos y/o implementaciones de SVE ampliar su alcance para que cubra las capas del proceso eleccionario.

Nuestra propuesta considera a la IR orientada por Objetivos, que permite desarrollar una visión holística del problema, abordando tanto factores humanos como tecnológicos y las relaciones entre estos [30], [31]. En particular, usamos el lenguaje de modelado *i** (*i-star*), que permite representar gráficamente las relaciones de dependencia entre un conjunto de actores (humanos y no humanos) con los objetivos que estos persiguen dentro del sistema que se intenta modelar [32]. En la Fig. 4 se muestra un *diagrama i** que permite modelar las dependencias a nivel estratégico (*i*-SD*). Un *diagrama i*-SD* ilustra la relación de dependencia entre los actores, sus objetivos (*goals* y *soft-goals*), las tareas que los actores realizan y los recursos necesarios. En nuestra propuesta se identifican 4 actores: gobierno, votante, observador y el SVE. El actor gobierno se refiere a la entidad de gobierno involucrada con la administración del proceso eleccionario, el actor votante representa a los ciudadanos, el actor observador se refiere a cualquier entidad independiente del gobierno y el actor SVE se refiere al conjunto de software, hardware y recursos humanos que sirven como medio para realizar el proceso eleccionario. Por otra parte los *goals* están relacionados directamente con los requisitos de la votación electrónica anteriormente mencionados mientras que los *soft-goals* están relacionados con los atributos de calidad recomendados.

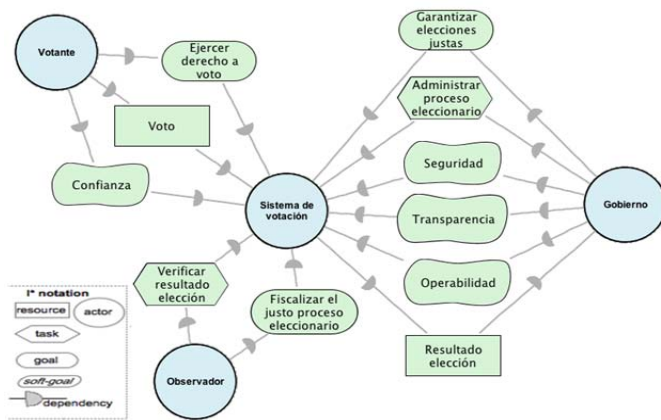


Figura 4. Diagrama i* SD system-to-be propuesto para un SVE [32]

C. Evaluación y amenazas a la validez

Después de haber conducido la búsqueda, se evaluó qué tan legítimos son los resultados obtenidos y consideramos que existen 2 principales amenazas a la validez de estos.

- Elección de subcaracterísticas

Se eligió no revisar las 27 características del ISO/IEC 25010:2011 en todas las publicaciones principalmente por restricciones de tiempo. Tratamos de mitigar esta amenaza considerando aquellas subcaracterísticas que están respaldadas por distintos trabajos, aún cuando no existe en la literatura algún trabajo que defina formal y explícitamente cuales son las subcaracterísticas más relevantes para los SVE.

- Conjunto acotado de fuentes para la búsqueda de trabajos

Existe un conjunto de trabajos relativos a los SVE que se encuentran indexados en fuentes no consideradas por este estudio. El no incluirlos se debe fundamentalmente a aspectos de alcance y tiempo disponible para el proyecto definido. Tratamos de mitigar esta amenaza considerando un subconjunto con fuentes de datos relevantes dentro del dominio de la IS (IEEE Xplore, ACM Digital Library y Science Direct).

V. CONCLUSIONES

Este trabajo ha presentado un mapeo sistemático que resume la presencia de RNF en propuestas de modelos y SVE.

Se pudo constatar que durante los últimos años ha existido un esfuerzo constante por mejorar los SVE, principalmente planteando modelos que sean más seguros y eficientes. De un total de 60 propuestas seleccionadas es posible establecer que al analizar los modelos y SVE bajo el marco del estándar ISO/IEC 25010, se observa una predominante presencia de la seguridad, seguida por eficiencia en el rendimiento de los sistemas.

Que la mayor cantidad de estudios se enfoque en los aspectos de seguridad de los SVE demuestra lo crítico que es para el éxito en la adopción de estos sistemas que sean dignos de confianza y puedan asegurar el cumplimiento de los requerimientos legales de las votaciones. Pese a que la seguridad es la mayor prioridad, preocupa que varios SVE utilizados sufran de serias fallas de diseño e implementación, siendo vulnerables a ataques maliciosos [33].

Los SVE deben generar confianza, tanto en los gobiernos que lo implementan como en los ciudadanos que lo usan. Para generar confianza se recomienda tener security como eje principal, es decir, partir construyendo el modelo buscando garantizar la integridad del sistema, luego en segundo lugar aparecen 3 características: Performance Efficiency y Reliability están para que el software sea adecuado cuando se utiliza en elecciones a gran escala, Operability está para poder garantizar que todos los usuarios puedan hacer uso del software con la menor necesidad de ayuda externa.

Considerando que una de las características del sufragio universal es que todos los ciudadanos habilitados puedan ejercer este derecho, resulta sorprendente que la evidencia revele que la accesibilidad es un tema ausente en las propuestas de SVE. Actualmente ningún sistema de votación sirve completamente a todos los votantes, hay reportes de elecciones que incluyendo SVE equipados con interfaces accesibles a personas discapacitadas no son implementadas o son implementadas de manera incorrecta en los lugares de votación [7].

Los resultados confirman a la seguridad como un RNF predominante de las propuestas estudiadas, lo cual es consistente con la literatura al señalar que es crítico para el éxito en la adopción de SVE y que garanticen a los votantes el resguardo de sus derechos constitucionales. Por otro lado los resultados muestran que los aspectos de seguridad en los SVE no están suficientemente desarrollados para poder satisfacer todos los requisitos impuestos, tanto en modelos teóricos como en sus implementaciones. Uno de los mayores potenciales de estos sistemas, la posibilidad de conducir elecciones con una frecuencia mucho mayor, no está siendo considerado actualmente. Acerca de la metodología empleada, el mapeo sistemático llevado a cabo es novedoso por cuanto hasta donde hemos revisado, no se han encontrado trabajos que lo apliquen al tema de SVE y RNF.

Como trabajo futuro se plantea ampliar las PI y fuentes consultadas. Dependiendo de estos resultados, realizar una revisión sistemática de literatura que permita hacer un análisis sobre la calidad de la evidencia recolectada.

AGRADECIMIENTOS

Este trabajo se desarrolló con el apoyo de la Vicerrectoría de Investigación y Postgrado de la Universidad de La Frontera, proyectos de Investigación DI14-0065.

REFERENCIAS

- [1] D. Budgen, M. Turner, P. Brereton, and B. Kitchenham, "Using Mapping Studies in Software Engineering," vol. 2, 2007.
- [2] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic Mapping Studies in Software Engineering," pp. 1–10, 2007.
- [3] International Institute for Democracy and Electoral Assistance, "Introducing Electronic Voting: Essential Considerations, 2011, no. December.
- [4] European Court of Human Rights, "European Convention on Human Rights," 2013. [Online]. Available: http://echr.coe.int/Documents/Convention_ENG.pdf
- [5] Council of Europe - Venice Commission, "Code of Good Practice in Electoral Matters," pp. 5–6, 2002. [Online]. Available: [http://www.venice.coe.int/webforms/documents/?pdf=CDLAD\(2002\)023-e](http://www.venice.coe.int/webforms/documents/?pdf=CDLAD(2002)023-e)
- [6] F. Yumeng, T. Liye, L. Fanbao, and G. Chong, "Electronic Voting: A Review and Taxonomy," 2012 International Conference on Industrial Control and Electronics Engineering, pp. 912–917, Aug. 2012. [Online]. Available:

- <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6322531>
- [7] S. Goodman, M. Mulder, and P. Smith, COUNTING VOTES 2012: A State by State Look at Voting Technology Preparedness, 2012.
 - [8] A. Kosmopoulos, "Aspects of Regulatory and Legal Implications on e-Voting," pp. 589–600, 2004.
 - [9] S. G. Weber, Coercion-Resistant Cryptographic Voting: Implementing Free and Secret Electronic Elections, 2008.
 - [10] G. Kotonya and I. Sommerville, Requirements Engineering: Processes and Techniques. John Wiley & Sons, 1998.
 - [11] IEEE Computer Society, "Guide to the Software Engineering Body of Knowledge - SWEBOK 3.0," 2013.
 - [12] I. Jacobson, G. Booch, and J. Rumbaugh, The Unified Software Development Process. Addison Wesley, 1999.
 - [13] J. Mylopoulos, L. Chung, and B. Nixon, "Representing and using nonfunctional requirements: a process-oriented approach," Software Engineering, IEEE Transactions on, vol. 18, no. 6, pp. 483–497, 1992.
 - [14] M. Glinz, "On Non-Functional Requirements," 15th IEEE International Requirements Engineering Conference (RE 2007), pp. 21–26, Oct. 2007. [Online]. Available: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4384163>
 - [15] ISO/IEC, "ISO/IEC 25010 - Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models," 2011.
 - [16] ISO-IEC, "ISO/IEC 9126 Software engineering — Product quality," 2001.
 - [17] J. Bryans, B. Littlewood, P. Ryan, and L. Strigini, "Evoting: dependability requirements and design for dependability," First International Conference on Availability, Reliability and Security (ARES'06), pp. 8 pp. –995, 2006. [Online]. Available: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1625415>
 - [18] G. Schryen, "Practical Security of Large-Scale Elections: An Exploratory Case Study of Internet Voting in Estonia," pp. 37–50, 2009.
 - [19] M. Volkamer, "Requirements for Remote Electronic Voting," in Evaluation of Electronic Voting, 2009, pp. 93–113.
 - [20] O. Spycher, R. Koenig, R. Haenni, and M. Schl'apfer, "Achieving Meaningful Efficiency in Coercion-Resistant, Verifiable Internet Voting," Electronic Voting, pp. 113–125, 2012.
 - [21] T. Dyb'a, "Strength of Evidence in Systematic Reviews in Software Engineering," in Second International Symposium on Empirical Software Engineering and Measurement (ESEM 2008), no. 7465, 2008, pp. 178–187.
 - [22] W. Afzal, R. Torkar, and R. Feldt, "A Systematic Mapping Study on Non-Functional Search-Based Software Testing," 20th International Conference on Software Engineering and Knowledge Engineering (SEKE), pp. 1–6, 2008.
 - [23] E. Benoist and B. Anrig, "Internet-Voting: Opportunity or Threat for Democracy?" pp. 29–37, 2007.
 - [24] O. Cetinkaya, "Analysis of Security Requirements for Cryptographic Voting Protocols (Extended Abstract)," 2008 Third International Conference on Availability, Reliability and Security, pp. 1451–1456, Mar. 2008. [Online]. Available: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4529515>
 - [25] K. Br'aunlich and R. Grimm, "A Formal Model for the Requirement of Verifiability in Electronic Voting by Means of a Bulletin Board," in E-Voting and Identify SE - 6, ser. Lecture Notes in Computer Science, J. Heather, S. Schneider, and V. Teague, Eds. Springer Berlin Heidelberg, 2013, vol. 7985, pp. 93–108. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-39185-9_6
 - [26] D. Foster and L. Stapleton, "Secure Remote Electronic Voting," 2004.
 - [27] L. Langer, A. Schmidt, J. Buchmann, M. Volkamer, and A. Stolfik, "Towards a Framework on the Security Requirements for Electronic Voting Protocols," 2010.
 - [28] S. Ikonopoulos, C. Lambrinouidakis, D. Gritzalis, S. Kokolakis, and K. Vassiliou, "Functional Requirements for a Secure Electronic Voting System," in Security in the Information Society SE - 40, ser. IFIP Advances in Information and Communication Technology, M. Ghonaimy, M. El-Hadidi, and H. Aslan, Eds. Springer US, 2002, vol. 86, pp. 507–519. [Online]. Available: http://dx.doi.org/10.1007/978-0-387-35586-3_40
 - [29] D. Lundin, "Component Based Electronic Voting Systems," pp. 260–273, 2010.
 - [30] E. Kavakli, "Goal-oriented requirements engineering: A unifying framework," Requirements Engineering, vol. 6, no. 4, pp. 237–251, 2002. [Online]. Available: <http://dx.doi.org/10.1007/PL00010362>
 - [31] S. Eric, P. Giorgini, and N. Maiden, Social modeling for requirements engineering. Mit Press, 2011.
 - [32] E. Yu, "Modelling strategic relationships for process reengineering," Ph.D. Thesis, Dept. of Computer Science, University of Toronto, 1995.
 - [33] A. F. N. Al-Shammari, A. Villafiorita, and K. Weldemariam, "Understanding the Development Trends of Electronic Voting Systems," 2012 Seventh International Conference on Availability, Reliability and Security, pp. 186–195, Aug. 2012. [Online]. Available: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6329181>



Samuel Sepúlveda es licenciado en Ciencias de la Ingeniería (1998) e Ingeniero Civil Industrial m. Informática (1999), por la Universidad de La Frontera, Temuco, Chile. Obtuvo su máster en Dirección y Gestión de Sistemas de Información y TIC, por la Universitat Oberta de Catalunya, España (2006). Actualmente postula al grado de Doctor en Aplicaciones de la Informática por la Universidad de Alicante, España. Se desempeña como profesor en el Dpto. de Cs. de la Computación e Informática, e investigador en el Centro de Estudios en Ingeniería de Software, Universidad de La Frontera. Sus intereses de investigación están en el área de Ingeniería de Software, Ingeniería de Requerimientos y Modelado de Líneas de Productos de Software.



Mauricio Bustamante es licenciado en Ciencias de la Ingeniería (2013) e Ingeniero Informático (2013), por la Universidad de La Frontera, Temuco, Chile. Actualmente se desempeña como desarrollador de aplicaciones para dispositivos móviles. Sus intereses de investigación están en el área de Ingeniería de Software y Desarrollos Ágiles.



Ania Cravero es licenciada en Ciencias de la Ingeniería (1996) e Ingeniera Civil Industrial m. Informática (1997), por la Universidad de La Frontera, Temuco, Chile. Obtuvo su máster en Tecnologías de la Información, por la Universidad Politécnica de Madrid, España (2006). Ha obtenido en 2010 su Doctorado en Cs. de la Computación y Sistemas Informáticos por la Atlantic International University, EE.UU.. Se desempeña como profesora en el Dpto. de Cs. de la Computación e Informática, e investigadora en el Centro de Estudios en Ingeniería de Software, Universidad de La Frontera. Sus intereses de investigación están en el área de Modelado Bases de Datos, Ingeniería de Requerimientos para Almacenes de Datos y Alineamiento de Objetivos.