

Evaluación de la integridad de datos en Sistemas de e-Voting

Silvia Bast¹; Germán Montejano ^{1 2}; Pablo García¹; Estela Fritz¹

¹Departamento de Matemática
Universidad Nacional de La Pampa
Av. Uruguay 151 – (6300) Santa Rosa – La Pampa – Argentina
Tel.: +54-2954-245220 – Int. 7125
[silviabast, pablogarcia, fritzem]@exactas.unlpam.edu.ar

²Departamento de Informática
Universidad Nacional de San Luis
Ejército de los Andes 950 – (5700) San Luis – San Luis – Argentina
Tel.: +54-2652-424027 – Int. 251
gmonte@unsl.edu.ar – web: <http://www.unsl.edu.ar>

Resumen

La incorporación de los sistemas de voto electrónico en las sociedades democráticas, parece surgir como una evolución natural dentro del proceso de transformaciones sociales que se está llevando a cabo actualmente. Sin embargo, el nivel de aceptación de este tipo de sistemas es sensiblemente menor que el de la mayoría de los servicios relacionados con gobierno electrónico. Para lograr la confianza de la población en esta tecnología, se deberá probar que los sistemas automáticos son confiables. A tal fin, se torna necesario focalizar en los aspectos que generan la mayor parte de los cuestionamientos en cuanto a su uso, entre los que se destaca la integridad y seguridad de los datos de los electores y de la elección en sí misma. El presente trabajo se propone evaluar la calidad de los datos de un conjunto de sistemas de voto electrónico. Para ello se toman como insumo: la característica de Seguridad del estándar internacional ISO/IEC 25010 y las características y sub-características de calidad de datos que especifica el estándar ISO/IEC 25012 y se hace uso de la estrategia GOCAME(Goal-Oriented Context-Aware Measurement and Evaluation)

para la medición y evaluación de los sistemas.

Palabras clave: *sistemas de voto electrónico, integridad de datos, seguridad, evaluación de la calidad.*

Contexto

El presente trabajo se enmarca en el Proyecto de Investigación: "Aspectos de Seguridad en Proyectos de Software", que se desarrolla en el ámbito de la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de La Pampa y en el Proyecto de Investigación "Ingeniería de Software, Conceptos, Métodos y Herramientas en un Contexto de Ingeniería de Software en Evolución" de la Universidad Nacional de San Luis.

Introducción

Si bien la promulgación de la Ley N° 8871, conocida también como la Ley Sáenz Peña estableció el voto y su sistema en la forma en que se conoce actualmente, la realidad de la sociedad de 1912 es totalmente diferente en la actualidad. Tal como se expresa en [1] "*Las tecnologías se presentan hoy como la encarnación de los valores de una so-*

ciudad democrática: la libertad, la igualdad y el intercambio", sin embargo aunque los servicios de gobierno electrónico se han popularizado mucho, no se observa el mismo nivel de aceptación en los sistemas de voto electrónico. Coexisten actualmente distintos tipos de sistemas eleccionarios:

- Tradicional: es el sistema propuesto en la Ley N° 8871 y que se aplica actualmente en la mayoría de las elecciones que se llevan a cabo en el país.
- Híbrido: Implica que alguno/s de los proceso/s se resuelven de manera electrónica y otro/s de forma manual. Tal es el caso de sistemas tales como: Wombat, Scantegrity y PunchScan
- Electrónico: todo el proceso eleccionario se lleva a cabo de forma electrónica. Tal es el caso de Helios y OpaVote, que además son sistemas totalmente online.

Características de los sistemas electorales

Por definición, el voto electrónico es un método en el cual los votos son emitidos o tabulados por medios electrónicos. Un sistema de voto electrónico es un componente de software que mapea el procedimiento de voto electrónicamente [2] y que debe cumplir además con un conjunto de requisitos [3], [4], [5] y [6] que le son propios y pueden resumirse en:

- *Secreto*: esto implica que el voto debe ser conocido únicamente por quién lo emitió
- *Autenticación del votante*: sólo las personas que figuran en el padrón de electores pueden emitir un voto
- *Verificabilidad*: debe ser posible verificar los siguientes aspectos: que los votos se contabilicen tal como se emitieron, que sólo los votos de electores habilitados se incluyan en el recuento final, que cada votante emita

un único voto y que el resultado del recuento final coincida con la voluntad de los votantes.

- *Simplicidad*: el sistema debe ser lo suficientemente sencillo e intuitivo como para que personas que no son expertas ni están en contacto cercano con la tecnología, puedan usarlo
- *Costo*: la adquisición, mantenimiento y operación del sistema debe poder realizarse a un costo razonable.
- *Auditabilidad*: El proceso electoral debe poder ser auditado en todas las etapas.
- *Inviolabilidad*: debe impedirse el cómputo parcial de la elección antes de la finalización del proceso eleccionario.
- *Seguridad*: debe ser imposible, para cualquier persona manipular los resultados de las elecciones.
- *No coerción*: se debe garantizar que los votantes no pasen por alguna de las siguientes situaciones: verse forzados a emitir votos inválidos, abstenerse bajo presión o que otra persona tome su lugar.
- *Robustez*: ninguna entidad debe interrumpir el proceso de voto.
- *Escalabilidad*: el esquema debe poder extenderse fácilmente para satisfacer requerimientos de computación, comunicación y almacenamiento de elecciones a gran escala.

Entre los requerimientos mencionados, existen algunos que no son fácilmente alcanzables y existen otros que parecen tener algunas contradicciones entre ellos, tal es el caso de verificabilidad, que requiere que se vinculen los electores a los votos y por lo tanto presenta una clara contradicción con la característica de Secreto.

Una de las principales causas de la desconfianza del electorado en los mencionados sistemas, radica en la percepción de que los datos pueden ser accedidos por terceras personas, que podrían rela-

cionar los votos con los electores o simplemente eliminarlos o modificarlos, y por lo tanto no se encuentran seguros.

Calidad del software y los datos en sistemas de voto electrónico

Con el fin de alcanzar los objetivos de integridad y seguridad, es menester tener en cuenta los estándares internacionales que se encuentran relacionados con la calidad de los sistemas de software y la calidad de los datos.

Considerando que los sistemas de voto electrónico son desarrollos informáticos puede probarse su adhesión a los estándares. ISO propone la norma 25010/2011 [7] referida a calidad en uso y a calidad de los productos de software. En ella se mencionan, para la categoría Calidad del Sistema, una serie de características: adecuación funcional, compatibilidad, usabilidad, confiabilidad, mantenibilidad, portabilidad y seguridad que es la que presenta mayor importancia a los efectos del trabajo. Esta última característica se divide en sub-características tales como: confiabilidad, integridad, no-repudio, responsabilidad y autenticidad.

Como además los sistemas de voto electrónico insumen y producen datos de extrema importancia, debe tenerse en cuenta el estándar internacional ISO/IEC 25012 de Calidad de datos [8], que propone dos puntos de vista para clasificar las dimensiones de calidad de datos:

- *Inherente*: se refiere a evaluar la calidad en cuanto al grado de satisfacción de las características del dato y concerniente a la satisfacción de las necesidades cuando el dato es usado bajo condiciones que han sido especificadas.
- *Dependiente del sistema*: enfoca la evaluación de la calidad teniendo en cuenta el dominio tecnológico en el que se utilizan los datos (dispositivos de hard-

ware, sistemas informáticos y otros programas).

Las características Inherentes que se mencionan en el estándar son: exactitud, completitud, consistencia, credibilidad y actualidad.

Existe además un conjunto de características que se consideran tanto Inherentes como dependientes del sistema: accesibilidad, conformidad, confidencialidad, eficiencia, precisión, trazabilidad y entendibilidad.

Las características dependientes del sistema son: disponibilidad, portabilidad y recuperabilidad.

En el presente trabajo se consideran relevantes: la característica de Seguridad del estándar internacional ISO/IEC 25010 y todas las características de calidad de datos incluidas en el estándar ISO/IEC 25012.

Dado que el objetivo es realizar un estudio comparativo de un conjunto de sistemas de voto, es necesario contar con una metodología que permita el análisis de cada uno de ellos.

Evaluación de la calidad de los sistemas

Para evaluar cada uno de los sistemas se hace uso de la estrategia GOCAME (Goal - Oriented Context - Aware Measurement and Evaluation) [9]. La misma sigue un enfoque orientado a objetivos y se define como de múltiples propósitos, dado que puede usarse para evaluar calidad de producto, sistema, sistema en uso, recursos, procesos, entre otros, instanciando los modelos de calidad adecuadamente.

Según sus autores, el primer paso en la aplicación de la estrategia GOCAME es definir la necesidad de información que intenta satisfacer requerimientos no funcionales de alguna de las categorías mencionadas en los modelos de calidad, para un propósito y un punto de vista de usuario particulares.

En este caso los modelos de calidad con los que se trabajará son el estándar in-

ternacional ISO/IEC 25010 en su característica de Seguridad y el estándar ISO/IEC 25012 en todas sus características. Cada una de las características incluye sub-características y atributos.

Para efectuar la medición se especifican métricas, que definen y explicitan de qué manera se obtienen los valores para los atributos. La evaluación se detalla e implementa usando indicadores que definen cómo se interpretan los valores de los atributos y calculan luego los conceptos de más alto nivel del modelo de calidad, posteriormente se hace un análisis de los valores obtenidos para realizar actividades de recomendación y toma de decisiones, que pueden implicar la sugerencia de mejora de la entidad evaluada o de otros cambios.

Debido a la variedad de sistemas de voto electrónico, se torna importante distinguir fortalezas y debilidades de cada uno de ellos para posteriormente realizar una propuesta superadora en cuanto a integridad y seguridad de los datos.

Líneas de Investigación, Desarrollo e Innovación

Las líneas de investigación que se siguen son:

- Evaluación y análisis comparativo de los tres tipos de sistemas: tradicional, híbrido y completamente electrónico, a través de las características y requerimientos que son propias de los sistemas electorales.
- Evaluación y análisis comparativo de un conjunto de sistemas de voto electrónico que se incluyen en la categoría de híbridos.
- Evaluación y análisis comparativo de un conjunto de sistemas de voto electrónico que se incluyen en la categoría de totalmente electrónicos.
- Elaboración de conclusiones que se desprenden del análisis previo.

- En base a las conclusiones obtenidas, presentar alternativas tendientes a garantizar la integridad de los datos.

Resultados y Objetivos

Se especificaron: la necesidad de información y las características, sub-características y atributos y sus respectivas métricas e indicadores que servirán para la realización del análisis comparativo entre los tres tipos de sistemas: tradicional, híbrido y completamente electrónico.

Se desarrollaron para los sistemas híbrido y totalmente electrónicos las necesidades de información y el detalle de características, sub-características y atributos que corresponden a los estándares ISO/IEC 25010 y 25012.

Actualmente se encuentra en desarrollo la fase de elaboración de indicadores para cada métrica de los atributos que se elaboraron y que corresponden a los estándares internacionales.

Se espera llevar a cabo la medición y la instanciación de los indicadores para posteriormente elaborar las conclusiones que surjan del estudio comparativo y presentar propuestas de mejoras a los sistemas en lo relativo a la integridad y seguridad de los datos.

Formación de Recursos Humanos

En el marco del presente proyecto se presentan los siguientes puntos relacionados con la formación de recursos humanos:

- Pablo García realizó una estadía de un año en la Universidade Federal de Minas Gerais (UFMG), aprobando seminarios de posgrado y trabajando en el grupo “Criptografía Teórica y Aplicada”, dirigido por Jeroen van de Graaf, PhD.
- Pablo García defendió su tesis para obtener el grado de Magister en Ingeniería de

Software de la Universidad Nacional de San Luis, bajo la dirección de Jeroen van de Graaf, PhD (UFMG) y Dr. Germán Montejano (UNSL). La tesis se tituló: “Optimización de un Esquema Dining Cryptographers Asíncrono” y recibió la calificación de sobresaliente.

- Silvia Bast está desarrollando su tesis para obtener el grado de “Especialista en Ingeniería de Software”. Su plan de trabajo fue aprobado y se planea su defensa para junio de 2015. La tesis se titula: “Sistemas de E-Voting: Integridad de Datos” y está dirigida por el Dr. Germán Montejano (UNSL) y el Magister Pablo García (UNLPam).
- Pablo García está desarrollando su tesis para obtener el grado de “Especialista en Ingeniería de Software”. Su plan de trabajo fue aprobado y se planea su defensa para septiembre de 2015. La tesis se titula: “Anonimato en sistemas de Voto Electrónico” y es dirigida por Jeroen van de Graaf, PhD (UFMG) y Dr. Germán Montejano (UNSL).
- Silvia Bast y Pablo García se encuentran cursando el Doctorado en Ingeniería Informática en la Facultad de Ciencias Físico Matemáticas y Naturales de la Universidad Nacional de San Luis (UNSL).
- Estela Fritz está desarrollando su tesis para obtener el grado de “Especialista en Tecnologías Informáticas aplicadas en Educación”. Su plan de trabajo fue aprobado y se planea su defensa para diciembre de 2015. La tesis se titula: “Propuesta de clasificación de software libre utilizado en la enseñanza de la

programación” y es dirigida por Mg. Alejandra Zangara (UNLP).

Referencias

- [1] **Busaniche, B., Heinz, F.** [et alt.] “Voto Electrónico: los riesgos de una ilusión” 1ra ed. Córdoba: Fundación Vía Libre ISBN 978-987-22486-5-9 Edición a cargo de Beatriz Busaniche y Federico Heinz, 2008.
- [2] **Odrisek, B.:** “E-Voting Security Study“-Communications-Electronics Security Group, X/8833/4600/6/21, (Copyright The Crown) Issue 1.2 31 United Kingdom, 2002
- [3] **Epstein, J.** “Electronic Voting”, Cyber Defense Agency LLC.
- [4] **Kazi Md. Alam Rokibul; Tamura, Shinsuke,** “Electronic Voting - Scopes and Limitations” IEEE/OSA/IAPR International Conference on Infonnatics, Electronics & Vision
- [5] **Prince, A.** “Consideraciones, aportes y experiencias para el Voto electrónico en Argentina”. 2005.
- [6] **van de Graaf, J., Henrich C., Müller-Quade, J.** ”Requirements for secure voting”. Notas de Trabajo. 2011.
- [7] **International Standard ISO/IEC 25010** Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models. 2011
- [8] **International Standard. ISO/IEC 25012** Software Engineering – Software Quality Requirements and Evaluation (SQuaRE) - Data Quality Model . 2008.
- [9] **Olsina L. Papa F., Molina H** “Modelling and Implementing Web Applications”, Rossi G., Pastor O., Schwabe D. &OlsinaL.“Cap.13 - How to Measure and Evaluate Web Applications in a Consistent Way.Springer-Verlag HCIS, London, 2008, 385-420