Título de la ponencia: Peligros formales sobre la utilización del voto electrónico por internet en la Universidad de Costa Rica

Proponentes: Elena Gabriela Barrantes Sliesarieva (elena.barrantes@ucr.ac.cr), Allan Francisco Berrocal Rojas (allan.berrocal@ucr.ac.cr), José Antonio Brenes Carranza (joseantonio.brenes@ucr.ac.cr), Edgar Casasola Murillo (edgar.casasola@ucr.ac.cr), Kryscia Ramírez Benavides (kryscia.ramirez@ucr.ac.cr), Alejandra Selva Mora (alejandra.selvamora@ucr.ac.cr), Ricardo Villalón Fonseca (ricardo.villalon@ucr.ac.cr), Escuela de Ciencias de la Computación e Informática.

Palabras clave: voto electrónico por internet, seguridad, fraude informático, democracia, sufragio

Eje temático: Gobernanza Institucional

Resumen Ejecutivo

Los sistemas de voto electrónico por internet son objeto de estudio en el área de computación y particularmente en seguridad informática. Se debe distinguir entre sistemas de voto apoyados por medios electrónicos, y sistemas de voto electrónico por internet. En los sistemas de voto electrónico por internet no existe garantía del cumplimiento de criterios de seguridad críticos, por lo que plantean una amenaza real contra la pureza del sufragio. En esta ponencia se listan y describen los aspectos

principales que garantizan la pureza del sufragio como derecho constitucional en nuestro sistema democrático. Además, se presentan los impedimentos técnicos que exhiben los sistemas de voto electrónico por internet como el sistema recientemente utilizado en la Universidad de Costa Rica. Se enumeran los riesgos derivados de la introducción de un sistema de voto electrónico por internet para reemplazar un sistema demostrablemente seguro, ampliamente utilizado y resguardado por las personas votantes como lo es el sistema de voto tradicional. Finalmente, se plantea una propuesta para la reglamentación de los sistemas de voto electrónico por internet en aras de proteger la robustez del sistema democrático en la Universidad de Costa Rica.

1. Justificación de la propuesta

En Costa Rica tenemos el privilegio de vivir en un sistema democrático reconocido como muy robusto a nivel nacional e internacional. Uno de los pilares de nuestro sistema democrático es el sistema de votación tradicional que garantiza la existencia de propiedades fundamentales como el anonimato, la seguridad y la confiabilidad en el proceso de emisión del sufragio. El sistema de votación tradicional (SVT) tiene la particularidad de que es supervisado o auditado en múltiples puntos por las mismas personas votantes que participan del proceso electoral. Así mismo, la dinámica del SVT es inclusiva, por cuanto esas mismas personas auditoras pueden tener o no tener afiliación con alguna de las candidaturas electorales. De hecho, la realidad de que en muchos casos las personas auditoras tienen afiliación o, al menos, afinidad con diferentes candidaturas, hace que su labor conjunta de supervisión dote de robustez al sistema como un todo.

Un sistema de voto electrónico (SVE) es un sistema de votación que se apoya en medios electrónicos en uno o varios puntos del proceso. Por ejemplo, se podría sustituir la papeleta impresa por una interfaz digital en una computadora en la cual la persona emite su voto y que, posteriormente, se imprime para que la persona lo deposite en una urna electoral. También se podría utilizar un sistema informático para que cada mesa electoral envíe digitalmente el resultado del conteo de votos al finalizar la jornada de votación. Estos, entre otros, son ejemplos de un sistema de votación apoyado por medios electrónicos para efectos de mejorar algún aspecto operativo dentro del flujo o dinámica de votación. Debe notarse que las características principales del SVT, ampliamente auditable, inclusivo y seguro, no se ven alteradas cuando se incluyen algunos elementos electrónicos en su flujo.

Por otra parte, un sistema de voto electrónico por internet (SVEI) es un sistema de votación diametralmente distinto a un SVT. La principal diferencia entre el SVEI y el SVT es que en el primero no existe la mesa de votación y, por ende, tampoco existe la posibilidad de que las personas votantes ejerzan un rol de supervisión o auditoría en el proceso de emisión del voto. En un SVEI es imposible garantizar el principio de anonimato del voto, algo que es parte esencial del proceso electoral en un sistema democrático. Para algunas personas esto podría ser poco relevante o podría, incluso, considerarse, de manera incauta, como una optimización o mejora para un SVT. Sin embargo, se puede demostrar que esta falencia en un SVEI formalmente impide garantizar principios fundamentales del derecho al sufragio, por lo cual, se puede inferir

que un SVEI no es equivalente a un SVT. En consecuencia, el uso de un SVEI crea un riesgo grave para la sostenibilidad del sistema electoral de la Universidad de Costa Rica, institución insignia y modelo de la democracia en Costa Rica.

2. Requerimientos esenciales para un sistema de votación

Los objetivos mínimos de seguridad e integridad que debe cumplir un sistema de voto electrónico secreto son: autenticación, anonimato, integridad de datos, auditoría, confidencialidad, integridad y disponibilidad del servicio, y seguridad en la interfaz del usuario. A continuación se presenta una breve descripción de cada uno siguiendo el trabajo de (Berrocal y Barrantes, 2007).

Autenticación: La autenticación se refiere a garantizar que sólo personas votantes legítimas puedan votar, que lo hagan sólo una vez, pero que siempre se les garantice el acceso a su oportunidad de votar.

Anonimato: En un sistema democrático el voto debe ser libre y secreto. Se debe garantizar que nadie, de ninguna manera, pueda asociar la identidad de la persona votante con su intención de voto. La garantía del principio de anonimato evita la coerción y evita la venta de votos.

Integridad de datos: Además de autenticar correctamente a las personas votantes y de mantener el anonimato del voto, es necesario garantizar que los registros de votos no sean modificados de ninguna manera, tal y como se garantiza cuando los votos son emitidos en una papeleta física y su integridad es supervisada por las personas que auditan el proceso.

Auditoría: En un sistema de votación es necesario garantizar que el sistema sea completamente auditable. Esto es fundamental en varias etapas del proceso como, por ejemplo, en el manejo de las papeletas que se distribuyen a las urnas de votación y que se le entregan a la persona votante, durante el resguardo que se da a los votos ya emitidos por las personas, durante la custodia de los votos en el trayecto de las mesas de votación hacia su recinto final, y también durante el conteo oficial de votos emitidos.

Confidencialidad, integridad y disponibilidad del servicio: Se refiere a la garantía del resguardo de todos los votos y demás datos producto de una votación, así como la disponibilidad del sistema en todo momento antes, durante y posterior a una votación.

3. Deficiencias y riesgos de un sistema de voto electrónico por internet

Los SVEI poseen al menos tres características tecnológicas y operativas que los vuelven inherentemente vulnerables al igual que otras aplicaciones de software que poseen estas características. La primera es que los SVEI se acceden mediante un navegador web, en computadoras o dispositivos electrónicos ordinarios como teléfonos portátiles, laptops y computadoras personales. Más allá de las vulnerabilidades de software que a menudo se descubren en los navegadores web, el principal problema de utilizarlos como parte de un SVE, es que es imposible equiparar un navegador web con el recinto privado que yace en las mesas de votación donde la persona votante puede emitir el sufragio de manera anónima y libre de coerción. La segunda característica vulnerable en el SVEI es el uso de la red de internet como canal de comunicación sobre el cual se transmite cada voto individual (sin respaldo físico como en papel) mediante mensajes electrónicos. El problema radica en que los mensajes

que viajan por la red de internet no están exentos de ser interceptados por un atacante que puede alterar la pureza de los votos. Finalmente, la tercera característica vulnerable de un SVEI es que el sistema principal que centraliza todas las funcionalidades, se hospeda en un servidor web que, como cualquier otra aplicación web, es vulnerable a una variedad inmensa de ataques informáticos, incluida la posibilidad de reemplazar totalmente la funcionalidad del SVEI por otro sistema malicioso que, incluso sin dejar rastro, altere los resultados de una votación.

Por lo anterior, es posible y, en muchos casos, relativamente fácil violentar los SVEI para impedir el cumplimiento de uno o más de los criterios de seguridad esbozados anteriormente. A continuación se describen algunos ejemplos.

Autenticación: Este objetivo se puede violentar fácilmente y sin mayores recursos tecnológicos en un SVEI con solo obtener la información de acceso de la persona votante y así suplantar su identidad. Es sabido que algunas personas tienen el mal hábito de compartir sus credenciales de ingreso a sistemas, o de no aplicar su debida custodia de manera secreta. En un SVEI esto vuelve imposible saber si un voto fue emitido por la persona misma o por otra persona que obtuvo acceso a sus credenciales. En consecuencia, quien obtiene el acceso, tiene acceso a votar, tenga o no derecho de hacerlo. Esto permite, de forma relativamente fácil, suplantar la identidad de algunas personas votantes y, de hecho, para algunas de estas personas, que no están habituadas a este tipo de sistemas, podría ser muy difícil o incluso imposible darse cuenta de que su identidad fue suplantada y que la intención de voto que él o ella emitió, nunca será contabilizada oficialmente. Adicionalmente, no hay forma de que una persona votante legítima pueda apelar si encuentra que su voto fue

alterado o que su identidad fue suplantada, ya que, debido a que no hay forma de probar un negativo en un SVEI, se imposibilita que el reclamo de una persona votante pueda acreditarse con evidencia.

Anonimato: Debido a que las personas emiten el voto de manera remota, sin la presencia de controles o la presencia de terceras personas imparciales, garantes de la pureza del proceso electoral, el principio de anonimato se puede violentar sin mayores dificultades ni recursos tecnológicos, simplemente obligando a la persona a emitir el voto frente al tercero (coerción), u ofreciendo emitir el voto frente al tercero (venta de voto). El SVEI le permite a la persona votante, así como a cualquier otra que esté a su lado, visualizar por quien está votando en cualquier lugar con acceso a Internet. Tanto la coerción como la venta de votos son problemas graves, y deben ser explícitamente evitados en cualquier SVE. El estándar internacional (COE-MD, 2017) indica claramente que en el caso del voto electrónico remoto se deben introducir provisiones que aseguren que el voto personal y libre sea respetado.

Un SVT posee la garantía implícita de que el voto es anónimo y secreto. En un SVEI sabemos entonces que no se puede garantizar ninguno de los dos, ni el voto secreto ni el voto anónimo. Un SVEI necesita autenticar a la persona votante precisamente para garantizar que el voto fue emitido por esta. Sin embargo, esto contradice el principio del voto secreto sobre todo si se considera que, como parte de un mecanismo de seguridad del sistema, debería ser factible inspeccionar o verificar que ningún voto haya sido alterado. Por lo tanto, la seguridad y el anonimato son principios difíciles o imposibles de satisfacer al mismo tiempo en un SVEI, cosa que sí es trivialmente posible en un SVT.

Integridad de datos: Para garantizar la integridad de los datos en un SVEI se necesitaría al menos independencia entre la empresa que desarrolla el SVEI, la empresa que lo opera durante un evento de votaciones electrónicas, la empresa que alberga los datos sobre los votos emitidos, y la empresa que realiza los cierres o contabilización de resultados. En un reporte reciente de la Unión Europea (CS-UE, 2023) se describen algunos SVE desarrollados a modo de programas piloto en algunos de sus países. Sin embargo, aún no se tiene conocimiento de ningún SVEI al que se le atribuyen todas las propiedades de seguridad expuestas aquí, incluso la de integridad de datos.

Auditoría: Un SVEI de origen propietario, por definición, no es trivialmente auditable en varios pasos del proceso considerados críticos. Se puede conseguir la auditoría de un SVEI si el sistema se desarrolla bajo un modelo de código abierto e integrando desde su concepción mecanismos que permitan la auditoría interna y externa del sistema, es decir, su auditoría a nivel estático y a nivel dinámico, durante su operación.

De acuerdo con los lineamientos del Consejo Europeo (COE-MD, 2017), en los ítems 33 y 39, a nivel de software de voto electrónico se debe contar con la posibilidad de auditar todo el proceso desde la instalación y configuración de los equipos, verificación de que la versión del código fuente del software utilizado en todos los diferentes equipos es la versión oficial no alterada del software del sistema, y la posibilidad de que personas expertas puedan revisar la totalidad el código fuente del sistema antes de su aprobación y uso. Esto permite a la ciudadanía depositar en personas expertas y conocedoras en la materia, su derecho fundamental de tener garantía y confianza de que el sistema de voto electrónico es seguro.

Confidencialidad, integridad y disponibilidad del servicio: Los alcances de un SVE en lo que respecta a la disponibilidad, confiabilidad, usabilidad y seguridad están descritos en (COE-MD, 2017) ítems 40 al 49. Se requiere un análisis a profundidad para verificar que un SVEI satisfaga dichos criterios. La disponibilidad del servicio es de importancia crítica y está asociada con la vulnerabilidad anteriormente descrita en relación a que un SVEI puede ser víctima de ataques informáticos que obstaculicen o impidan completamente su uso.

4. Propuesta para la Universidad de Costa Rica en relación con el uso de SVEI

    1. Modificar el Reglamento de Elecciones Universitarias, artículos 31 y 32 para prohibir de manera explícita el uso de sistemas de votación electrónica por internet (SVEI) para la elección de miembros del Consejo Universitario en la Universidad de Costa Rica.

    2. Modificar el Reglamento de Elecciones Universitarias, artículo 34 para prohibir de manera explícita el uso de sistemas de votación electrónica por internet (SVEI) para la elección del Rector o Rectora de la Universidad de Costa Rica.

    3. Modificar el Reglamento de Elecciones Universitarias, agregando un artículo para prohibir de manera explícita el uso de sistemas de votación electrónica por internet (SVEI) para todo proceso electoral en la Universidad de Costa Rica, salvo casos justificados a solicitud del(a) votante, como por ejemplo la votación vía medios electrónicos para procesos ordinarios en centros, institutos o unidades académicas, o de fuerza mayor, listados de manera explícita, y cuyas características impidan la realización de un proceso de votación tradicional.

Referencias

1. (Berrocal y Barrantes, 2007) Berrocal, A. & Barrantes, G. (2007). Consideraciones de Seguridad para la Implementación de un Sistema de Voto Electrónico en Costa Rica. *Tiempo Compartido*, 7(3), 12-21. [Enlace]
2. (COE-MD, 2017) Comité de Ministros del Consejo Europeo. Directrices sobre la aplicación de las disposiciones de la Recomendación CM/Rec(2017)5 sobre normas para el voto electrónico. Comité ad hoc de expertos en normas jurídicas, operativas y técnicas para el voto electrónico (CAHVE) [Enlace]
3. (CS-UE, 2023) Comisión de Servicios de la Unión Europea. Compendio sobre voto electrónico y otras prácticas en tecnologías de la información y comunicación. (2023). ISBN 978-92-68-09554-6. Doi: 10.2838/464803 [Enlace]