Votación electrónica remota para la Universidad de Chile

ALEJANDRO HEVIA

Académico del Departamento Ciencias de la Computación de la Universidad de Chile. Coordinador Académico en Participa UChile, y director del Laboratorio de Criptografía Aplicada y Ciberseguridad, CLCERT, Universidad de Chile. Doctor en Ciencias de la Computación por la University of California, San Diego, Estados Unidos.

ahevia@dcc.uchile.cl

CAMILO GÓMEZ

Magíster en Ciencias de la Computación por la Universidad de Chile. Coordinador Operativo en Participa UChile.

cjgomez@uchile.cl

CATALINA BURGOS KREITHER

Diseñadora Gráfica por la Universidad del Pácífico. Diseñadora Gráfica en Participa UChile. En Twitter la encuentras como @catalina_bk.

MARTA APABLAZA

Licenciada en Historia por la Universidad de Chile y Periodista por la Universidad Católica. Encargada de comunicaciones en Participa UChile.

marta.apablaza@gmail.com

Investigadores de la Facultad de Ciencias Físicas y Matemáticas desarrollaron un sistema de votación electrónica remota para ser utilizado por toda la comunidad universitaria, que puede tener un impacto de largo alcance en cómo se ejercita la democracia en pequeñas comunidades.

La interrupción de nuestra vida cotidiana debido a la pandemia fue un evento que dejó grandes interrogantes respecto a cómo ejercemos ciertos hitos políticos de nuestra vida cotidiana como lo son elecciones y derecho a voto en espacios comunitarios. ¿Cómo crear y ejercer un sistema de votación electrónica de forma remota y segura? La respuesta a esta interrogante la está construyendo Participa UChile, en la forma de un nuevo sistema de votación electrónica remota universitaria, impulsado por la Prorrectoría de la Universidad de Chile, cuyo desarrollo está a cargo de un grupo de investigadores de la Facultad de Ciencias Físicas y Matemáticas (FCFM), y que cuenta con el apoyo técnico de la Vicerrectoría de Tecnologías de la Información (VTI).

Este nuevo sistema fue diseñado para ser utilizado en la mayoría de los procesos de votación al interior de la Universidad de Chile, tales como elecciones de decanos, directores de departamentos, centros de estudiantes y representantes de personal de colaboración, entre otras. Al ser un sistema de votación electrónica remota, los integrantes de la comunidad universitaria pueden sufragar desde un computador, un teléfono o una *tablet*, sin necesidad de recurrir físicamente a un recinto de votación. Cabe destacar que para ingresar al sistema de votación, las personas solo requieren tener activa su cuenta institucional (Pasaporte UChile).

El desarrollo de este proyecto comenzó en marzo de 2021 buscando expandir las opciones de participación dentro de la comunidad universitaria sin dejar de cumplir los niveles de seguridad y confiabilidad asociados a nuestra Universidad.

¿En qué consiste Participa UChile?

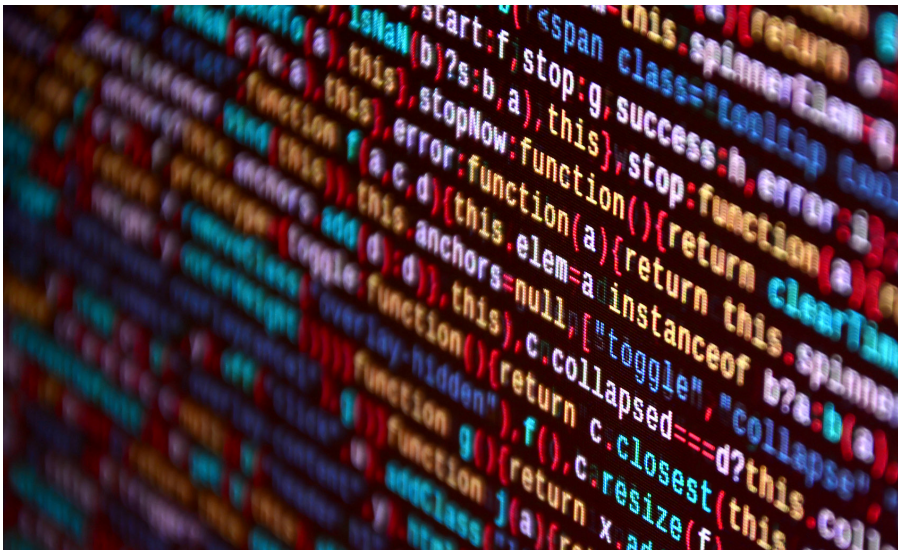
Participa UChile (https://participauchile.cl/) está basado en Helios, un sistema de votación electrónica remota y verificable para votaciones de bajo riesgo (https://vote.heliosvoting.org/). Fue creado en 2008 por Ben Adida, por entonces estudiante de doctorado en criptografía en MIT, quien lo desarrolló como un sistema de código abierto. Este acceso público no solo permite a quien quiera conocer cómo fue construido sino además tomar ese código, utilizarlo y modificarlo.

El profesor Alejandro Hevia, académico del Departamento de Ciencias de la Computación y director del Laboratorio de Criptografía Aplicada y Ciberseguridad (CLCERT) de la FCFM, lidera el equipo de desarrollo de Participa UChile. "Helios es un sistema diseñado y mejorado por expertos, que ha sido utilizado por importantes entidades como la Asociación Internacional de Investigación Criptográfica y por universidades como Princeton en Estados Unidos y la Universidad Católica de Lovaina en Bélgica", explica. Y agrega: "Su uso previo en un contexto académico, y el ser de código abierto, nos da la confianza que ha sido revisado, testeado y mejorado desde su creación. Es entonces un sistema probado que adaptamos para nuestro contexto universitario". Destaca que Helios utiliza criptografía, lo que permite garantizar el secreto del voto. En términos simples, esto significa que se emplean técnicas matemáticas que permiten "sellar" el voto, o en términos técnicos "cifrarlo", lo que impide que una persona distinta al votante pueda ver o modificar su contenido, incluso si se trata del administrador del sistema.

En el caso particular de Participa UChile, se agregaron también funcionalidades específicas requeridas por reglamento, como la posibilidad de emitir voto ponderado, o poder votar nulo o blanco.

[Participa UChile] fue diseñado para ser utilizado en la mayoría de los procesos de votación al interior de la Universidad de Chile, tales como elecciones de decanos, directores de departamentos, centros de estudiantes y representantes de personal de colaboración.

El profesor Alejandro Hevia indica que Participa UChile está diseñado —inicialmente— para llevar a cabo elecciones dentro de la comunidad universitaria. Esto, porque al tratarse de un ambiente con bajo riesgo de ataque informático se pueden practicar diferentes formas de elección e ir mejorando en seguridad y procesos. "En elecciones comunitarias los incentivos económicos o de otro tipo para perjudicar la elección son acotados y manejables". Sin embargo, agrega el académico, los desafíos son significativos incluso en este escenario. "Las elecciones comunitarias aun cuando sean pequeñas o medianas también requieren dar garantías de privacidad, integridad, transparencia y usabilidad", indica el profesor Hevia, al tiempo que clarifica su objetivo: "Participa UChile busca resolver el problema de las elecciones y consultas seguras en forma científica, paso a paso, construyendo sistemas que combinan la teoría y la práctica, desde situaciones de bajo riesgo, en forma sistemática, robusta, y participativa".



Al basarse en el software Helios, una plataforma usada y testeada extensivamente, y ser de código abierto, Participa UChile entrega la posibilidad de auditar errores y realizar las mejoras necesarias en forma transparente.

Ventajas de una elección remota con fundamentos criptográficos

La utilización de técnicas criptográficas en Participa UChile permite entregar tres importantes garantías a sus usuarios: secreto del voto, mitigación de la coerción y realización de auditorías online.

Respecto al secreto del voto, en general, en otros sistemas de votación electrónica este depende en gran medida de la probidad de los administradores del sistema, quienes eventualmente podrían acceder al servidor y conocer quiénes votaron y por qué candidato. Participa UChile innova en este aspecto, ya que el secreto del voto depende de los llamados *custodios de clave*.

Este último concepto es un símil a los tradicionales vocales de mesa: son un número pequeño de personas, encargadas de realizar el conteo final de votos. Para esto, los custodios comparten una clave privada que crean especialmente para la votación y que tiene la particularidad que ningún custodio por sí solo puede abrir esta urna virtual.

El sistema está diseñado para "dividir" la clave en trozos, uno para cada custodio y, por lo tanto, requiere que los custodios ingresen su clave en forma conjunta. En otras palabras: "Esto es similar a una puerta con tres candados de seguridad donde la llave de cada candado la tienen tres personas distintas. Una sola persona puede abrir su candado, pero si el resto no lo hace la puerta seguirá cerrada. En nuestro ejemplo, necesitaríamos de las tres llaves para abrirla. Si bien esto es bueno, permitiría a una persona boicotear el proceso si se niega a abrirla. Por eso, nuestro sistema va más allá y permite 'abrir la puerta', esto es realizar el conteo, siempre que al menos dos de los tres los custodios participen. Eso agrega solidez al sistema", explica el profesor Hevia.

En la práctica, los custodios de clave deben ser designados (o posiblemente elegidos) en forma previa a cada elección.

Camilo Gómez, coordinador operativo de Participa UChile, profundiza: "Nuestra propuesta es que sean tres a cinco 'custodios de clave', según la elección. Si bien desde el punto de vista técnico no hay problema en designar una cantidad mayor, un número más amplio podría hacer más complejo coordinar su labor y eventualmente afectar las garantías del sistema. Con todo, esta es solo una sugerencia de operación, y la junta electoral es quien debiera tomar la decisión final".

Además de mantener el secreto del voto, Participa UChile mitiga la coerción, es decir, que alguien obligue al votante a marcar una determinada preferencia. La solución es permitir votar más de una vez, pero preservando la unicidad del voto. Si un votante decide cambiar su preferencia una vez emitido su voto puede ingresar a la plataforma y votar nuevamente, sobrescribiendo ese nuevo voto al anterior. Es decir, se puede reemitir el voto mientras el proceso esté abierto, pero solo se cuenta el último voto. "Esta estrategia es considerada por la comunidad científica como una mitigación razonable para el problema de la coerción", explica Alejandro Hevia.

La tercera garantía que otorga Participa UChile tiene que ver con la realización de auditorías online. El sistema permite que, mientras se están emitiendo los votos e, incluso, mientras el sistema está contándolos, se pueda verificar externamente que cada uno

de los pasos se ha ejecutado correctamente sin comprometer el secreto de los votos ni las claves de los custodios. El truco está en la existencia de algoritmos matemáticos que operan sobre valores públicos emitidos por el sistema, permitiendo "testear" que todos los votos válidos fueron considerados, y que los custodios operaron correctamente. Esta auditoría indirecta permite tener certeza sobre la integridad del cómputo final y, eventualmente, detectar si alguien intentó modificar el resultado.

Roles en una elección

Al igual que en una elección presencial, donde existen vocales de mesa y encargados de recintos de votación, Participa UChile considera roles y actores definidos para cada elección: Junta Electoral, administrador del sistema, custodios de claves y votantes.

La Junta Electoral es el equivalente al Tricel del Servel para una elección específica. El reglamento universitario establece que debe existir una para toda elección; si bien su composición depende del tipo de elección, debe supervisar la correcta realización del proceso de votación según lo establecido en el reglamento, e informar sobre la fecha de votación, candidatos y universo de votantes, entre otras tareas.

El administrador de sistema es el encargado de la configuración de la elección de acuerdo con lo especificado por la Junta Electoral. Este rol lo ejercen los encargados de Participa UChile, actualmente el profesor Alejandro Hevia y Camilo Gómez.

"Los custodios, como se mencionó anteriormente, son los encargados de las claves y se designan o eligen en forma previa a una elección y solo para ella. Es importante destacar que los custodios de clave no tienen por qué ser los administradores. Un custodio es un equivalente al vocal de mesa, con la diferencia que en vez de estar presentes todo el proceso de elección, solo deben hacerlo en dos oportunidades: antes de abrir la votación para crear las claves, situación equivalente a constituir mesa. Y al cierre del proceso, para abrir la urna y realizar el conteo de votos", explica el profesor Hevia.

La utilización de técnicas criptográficas en Participa UChile permite entregar tres importantes garantías a sus usuarios: secreto del voto, mitigación de la coerción y realización de auditorías online.

Riesgos y mitigación

Los investigadores a cargo del desarrollo de Participa UChile explican que todos los sistemas de votación electrónica remota presentan riesgos inherentes. Sin embargo, aclaran, también los mecanismos utilizados para mitigarlos en el caso particular del sistema de la Universidad de Chile.

Un riesgo ya mencionado tiene que ver con la coerción. Si bien en Participa UChile el riesgo se mitiga, no se elimina. Tal como explica Camilo Gómez, "el sistema no puede evitar que alguien te presione externamente a votar por una opción determinada. Tampoco previene la venta del voto. A nivel mundial, no existe sistema de votación remoto o presencial que lo prevenga completamente; es un problema que las democracias modernas están abordando". La estrategia de reemitir el voto, al menos por ahora, parece ser la opción más efectiva.

Un segundo riesgo tiene que ver con fallas provocadas por ataques informáticos, o lo que comúnmente se conoce como "*hackeos*". Por ejemplo, alguien

Todos los sistemas de votación electrónica remota presentan riesgos inherentes.

podría crear un virus que ataque el computador o tablet del votante, de modo que, si emite preferencia por el candidato A, el sistema por atrás "marque" el candidato B sin que el votante sepa. También está la posibilidad de ataques masivos que buscan interrumpir la conectividad de los votantes, tales como el corte de los cables de fibra óptica o ataques de denegación de servicios con los cuales se impide el acceso al servidor de votación. Todo esto podría impedir el acceso del votante a la plataforma de votación.

Otro ataque tiene que ver con *hackear* el servidor donde se almacenan los votos. Tal acción, si bien disruptiva, en Participa UChile tendría un efecto limitado. Gracias a que los votos están encriptados y las claves de los custodios no se almacenan en el servidor, el atacante no podría conocer por quién votó cada persona. "Entonces en términos del secreto del voto, este no se ve afectado, aunque sí podría obligar a realizar nuevamente todo el proceso de votación", indica Gomez.

Alejandro Hevia afirma que, para el ámbito de acción de Participa UChile, este tipo de ataques masivos no debieran ocurrir: "Crear un virus efectivo, por ejemplo, requiere de conocimiento y financiamiento. Nuestra apuesta es que, en un entorno comunitario como el universitario, la existencia de personas o grupos dispuestos a este esfuerzo o gasto es menos probable, versus en una elección de alto riesgo como la de presidente o parlamentarios".

Si bien estos son riesgos inherentes a todos los sistemas de votación electrónica, reitera que "en nuestro caso de uso, los incentivos no están alineados para que los participantes u observadores quieran llevar a cabo estos ataques masivos y toman preponderancia otros riesgos menores tales como coerción ocasional simple, inyección o manipulación de votos, o un custodio/administrador curioso, todos los cuales son cubiertos razonablemente en Participa UChile". En cualquier caso, expresa el profesor Alejandro Hevia, "la comunidad debe saber que los riesgos más severos, si bien no son esperables, efectivamente existen".

Beneficios

Uno de los aspectos fundamentales de Participa UChile es entregar confianza frente a posibles riesgos. Para combatir las posibles fallas del sistema, Alejandro Hevia destaca el hecho que, al basarse en el software Helios, una plataforma usada y testeada extensivamente, y ser de código abierto, Participa UChile entrega la posibilidad de auditar errores y realizar las mejoras necesarias en forma transparente. "Esto es una medida de protección. El código está disponible para que cualquier persona pueda mirarlo y si tiene dudas pueda preguntarle a su amigo experto en programación u otra persona que sepa de criptografía, porque la idea es que el proyecto sea lo más transparente posible. Así, cualquier error o falla que alguien pueda encontrar, esperamos que nos la reporten para nosotros arreglarla. Esperamos con eso seguir el ejemplo de Helios, sobre el cual si bien se detectaron fallas, estas se corrigieron".

Otro beneficio de la votación electrónica entregada por Participa UChile, además de no requerir presencia física en una votación, es el potencial de especialización de los votos, por ejemplo: utilizar idiomas distintos o incluir en el voto preguntas de una mayor complejidad de lo que permite el voto en papel. "Se puede solicitar ordenar opciones según una preferencia. Si incorporamos tales mecanismos, que permitan capturar preferencias más complejas de la comunidad, tenemos el potencial de mejorar la representatividad y legitimidad de las elecciones o decisiones tomadas usando el sistema", indica.

Asimismo, los beneficios de desarrollar una votación electrónica y remota de manera segura se pueden extender más allá del tiempo y de las complejidades de los últimos años donde la cotidianidad se ha visto interrumpida por la pandemia: "Podemos comenzar a ejercitar una forma de votación y ejercer derechos totalmente nueva y podemos empezar a crear conocimiento y confianza en este tipo de sistemas", señala Hevia.

"Construir un sistema de votación electrónica con altos estándares de seguridad en el ámbito técnico y que cuente con la confianza de los electores es un proceso de largo aliento. En Participa UChile estamos invitando a la comunidad a participar para seguir creciendo en seguridad y transparencia en este sistema", finaliza Hevia. ▪