

Buenos Aires Censuró y Allanó A Quienes Reportaron Falencias del Voto Electrónico

July 15, 2015 | By David Bogado and Danny O'Brien

La ciudad de Buenos Aires está en proceso de elegir a su próximo Jefe de Gobierno y a los miembros de la Legislatura. Las elecciones fueron el [pasado 5 de julio](#), cuyos resultados derivaron a una segunda vuelta programada para el 19 del corriente, al mismo tiempo, debutó en la capital Argentina un sistema de votación electrónica denominado [Vot.ar](#), desarrollado por la compañía [Magic Software Argentina \(MSA\)](#).

Como tantos otros sistemas electrónicos de votación en el pasado, la seguridad y la transparencia del sistema [Vot.ar](#), implementado en elecciones anteriores en las provincias de Salta y Córdoba, ha sido puesto en cuestionamiento por técnicos informáticos locales, abogados, defensores de derechos humanos y usuarios de Internet desde su lanzamiento original. Un problema en versiones anteriores de [Vot.ar](#) fue [un simple hack](#) que transformaba la boleta electrónica en una llave que daba acceso de administrador a un usuario de la máquina de votación, permitiéndole recalibrar la pantalla táctil y engañar a los votantes para que elijan a otro candidato.

Pero en vez de tomar nota de las falencias o posponer la implementación de [Vot.ar](#), las autoridades de la ciudad de Buenos Aires eligieron el silencio, la intimidación a los críticos de los problemas no resueltos del sistema, el bloqueo a sitios web y el allanamiento con secuestro de pertenencias de un tecnólogo y profesor local, [Joaquín Sorianello](#), que reportó a MSA una falencia clave en su ya montada infraestructura. Incluso mientras las elecciones continúen con las fallas tecnológicas, la información en línea de los problemas resulta legalmente censurada a los lectores,

así como la vida y las pertenencias de Sorianello siguen en el limbo.

El sistema [Vot.ar](#) se basa en una [boleta electrónica](#) con chip RFID incorporado. Cada votante [inserta la boleta](#) en una máquina de votación y registra su preferencia mediante una pantalla táctil. El voto se imprime en la boleta y (en teoría) también se almacena en el chip RFID incrustado. Para el escrutinio se recogen las boletas junto a sus chips usando los mismos equipos de MSA para la verificación y los recuentos, y se transmiten los datos de cada mesa de los locales de votación a un centro de cómputos.

Las críticas a [Vot.ar](#), se hicieron más constantes en los días previos a las elecciones en Buenos Aires. A fines del mes de Junio, Sorianello se comunicó con MSA para reportarles que los certificados SSL privados, utilizados para la transmisión segura de datos entre los centros de votación y el de cómputos, se encontraban accesibles al público. Un adversario con acceso a estos certificados podría monitorear o manipular los resultados enviados a las autoridades. Otro [grupo de investigadores independientes](#) descubrió que con un teléfono inteligente [con capacidad NFC](#) podrían agregar múltiples votos del mismo candidato en el chip RFID de la boleta electrónica, alterando invisiblemente el resultado del escrutinio.

La respuesta de las autoridades no fue investigar el riesgo de los problemas, sino ocultar la evidencia y castigar a los informantes. El 3 de Julio, dos días antes de las elecciones, la división de delitos informáticos de la Policía Metropolitana de Buenos Aires, bajo las órdenes de la Jueza María Luisa Escrich, allanó la residencia de Sorianello. Los funcionarios requisaron sus computadoras, sus lectores de libros electrónicos Kindle y otros dispositivos. El informático no estaba presente en su residencia al momento del allanamiento, pero en una [conversación telefónica con un medio local](#), declaró que "si quisiera hackear o hacer algo dañino no le hubiera avisado a la empresa".

El mismo día del allanamiento, la Jueza Escrich, en un intento de limitar las filtraciones, ordenó a los proveedores de servicios de Internet de Argentina proceder "al inmediato bloqueo" del acceso a

cinco URLs de justpaste.it, uno de los sitios donde la información del sistema [Vot.ar](https://vot.ar) era difundida. La [información sobre la censura](#) se hizo pública luego de la primera vuelta de las elecciones.

[Fundación Vía Libre](#), organización no gubernamental argentina que desde el año 2000 promueve el uso del software libre, el derecho a la privacidad y la defensa de los derechos digitales, ha [advertido con antelación](#) sobre los riesgos de la adopción de un sistema vulnerable.

Enrique Chaparro, su director, contó a EFF:

(El sistema) [Vot.ar](https://vot.ar) gira en torno al almacenamiento de datos de la boleta en los chips RFID. Se ha demostrado que esta tecnología es insegura en varias ocasiones y eso llevó a Israel a dejar de lado un sistema idéntico en el año 2009. El proceso de adquisición estuvo sesgado y fue inusualmente rápido para cualquier estándar (15 días para la licitación y 4 días para la evaluación).

[Beatriz Busaniche](#), Directora de Vía Libre, agregó:

Toda la implementación del voto electrónico se hizo a través de un Decreto Ejecutivo del Gobierno de la Ciudad de Buenos Aires, mientras que la ley establece que para el uso del voto electrónico, se necesita una mayoría calificada (Ley 4894, Anexo II, art. 25). El código fuente de [Vot.ar](https://vot.ar) no se puso a disposición del público y no existieron auditorías independientes, basados en la premisa que MSA no podía mostrar el código por motivos de seguridad.

En la primera ronda electoral de Buenos Aires, los votantes ejercieron su derecho a través del sistema [Vot.ar](https://vot.ar) con poco conocimiento de sus problemas hechos públicos y los intentos de silenciar a sus críticos apenas unos días antes. Según la prensa local, 500 de las máquinas de votación [no pudieron transmitir sus resultados](#) al centro de cómputos, dando lugar a 184.317 votos que fueron finalmente incluidos solamente después de un recuento físico. La ciudad de Buenos Aires cuenta con más de 2.5 millones de votantes.

La EFF ha seguido de cerca otros casos relacionados con el desarrollo del voto electrónico donde investigadores han sido objetivos o han sido criticados por exponer las vulnerabilidades del sistema. En India, país con las elecciones más extensas en el mundo, el investigador en seguridad informática Hari Prasad y sus colegas Alex Halderman y Rop Gonggrijp [habían descubierto severas fallas](#) en las máquinas electrónicas de votación (electronic voting machines en inglés, EVM) que permitían cambiar los resultados y comprometer el secreto del voto en el año 2010.

Por su trabajo, Prasad fue acusado penalmente por supuesto robo de una máquina de votación, quedando detenido en Mumbai por una semana y luego liberado bajo fianza. EFF galardonó a Prasad con el [Pioneer Award de 2010](#) por hacer su trabajo frente al acoso legal, y por hallar las falencias en un sistema que podía socavar el funcionamiento democrático de su país.

Este año, el profesor Halderman y la investigadora de la Universidad de Melbourne Vanessa Teague descubrieron [una falla en el cifrado del sistema](#) de votación electrónica en el estado de New South Wales en Australia, que pudieron haber dejado unos 66 mil votos vulnerables a la vigilancia y a la manipulación en las más recientes elecciones a nivel de estados. Un alto funcionario de la Comisión Electoral de New South Wales intentó desacreditar el trabajo de Halderman y Teague como parte de una campaña tendenciosa contra el voto electrónico, pero finalmente admitieron los riesgos y modificaron sus sistemas para hacer frente a las debilidades.

El sistema [Vot.ar](#), como lo es operado actualmente, carece de los requisitos básicos en transparencia, seguridad y rendición de cuentas. Así como en India y en Australia, críticos en público como Sorianello y otros permanecen como la mejor defensa frente a las autoridades argentinas. Y, sin embargo, los funcionarios y los jueces han optado por sostener su deficiente tecnología en lugar de buscar más revisión pública.

MSA, la Ciudad de Buenos Aires y la Jueza Escrich deberían corregir sus propios errores. Deberían dar marcha atrás una investigación infructuosa y perjudicial, y tratar a los expertos y

expertas en informática del país con respeto, no con allanamientos y censura en Internet, por el trabajo que han hecho para proteger la democracia y el futuro del voto electrónico. Tienen muchos problemas que resolver en los días previos a la segunda vuelta electoral, no cuentan con tiempo ni la credibilidad para perturbar legalmente a los voluntarios que los ayudan a corregir el desastre del voto electrónico de su ciudad.

Varias fuentes anónimas han colaborado para este material. A ellos/as, muchas gracias.