Tiempo de votaciones, ¿son confiables las urnas electrónicas?

➢ *Por staff de redacción Infosecurity Mexico.*

El mundo gira en torno a los cada vez más sofisticados dispositivos electrónicos personales, el acceso a internet en cualquier lugar y a la inmediatez para conseguir información, comunicarse y comprar. Se calcula que existen alrededor de 15.140 millones de dispositivos *IoT* conectados globalmente, y se piensa que se duplicarán para el año 2030[1]. En enero de 2023 México tenía una población en línea de aproximadamente 100.6 millones de usuarios y más de 96.47 millones de usuarios de internet móvil[2].

Sin embargo, uno de los procesos que en muchos países no ha logrado establecerse completamente de manera electrónica son las votaciones para elecciones gubernamentales, aunque la tendencia es cada vez mayor en adoptar nuevas tecnologías y sistemas electrónicos para realizarlas. En América, tanto Brasil como EE. UU[3]. han implementado este sistema, no obstante, la implementación ha sido desigual.

Puede parecer increíble que, mientras la tecnología influye cada vez más en nuestra vida y actividades diarias, el uso de medios electrónicos para elecciones o consultas aún no se ha difundido de forma masiva. Lo cierto es que en México se irá utilizar parcialmente, o de manera paralela, en las próximas elecciones del Estado de México, el próximo cuatro de junio[4].

De acuerdo con expertos, el escaso uso de esta modalidad se debe principalmente a la desconfianza que genera en muchas personas la duda de que los votos sean realmente libres, confiables, secretos y seguros, ya que consideran que es fácil que un sistema computarizado pueda ser vulnerado y altere el voto personal o el resultado final[5].

Sin embargo, cabe señalar algunas ventajas que ofrecen los sistemas electrónicos para votar:

- Celeridad en el proceso.
- Ahorro de recursos en logística y material desechable.
- Menor carga de trabajo para funcionarios electorales.
- Posibilidad de votar desde cualquier lugar y no en una casilla específica.
- Rápida obtención y difusión de resultados.

Aunque, desde luego, también hay desventajas en un proceso electrónico:

- Altos costos de los equipos que deben instalarse en las casillas para el proceso.
- Probabilidad de manipulación si no se toman medidas de seguridad adecuadas.
- Escasa confianza de los electores y partidos políticos.

Este último es precisamente el principal escollo para implantar este tipo de sistemas, pues en una elección tradicional se cuentan los votos físicos para verificar los resultados, mientras que en un sistema electrónico hay temor de que se alteren los resultados por parte de los organizadores, el gobierno o los piratas cibernéticos que pudieran afectar el proceso.

Es decir, aun con tecnología de punta, existe la posibilidad de algún imprevisto por los riesgos

---

[1] https://bit.ly/3IkZpFh
[2] https://bit.ly/2nRzrQk
[3] https://bit.ly/3MzTGgb
[4] https://bit.ly/3MBmMgd
[5] https://bit.ly/3pFCxcT

del sistema o por el uso de los dispositivos electrónicos, por lo que se debe contar con un plan de respuesta que contemple un mapa de riesgos con soluciones inmediatas para no impactar el proceso, además del apoyo de sistemas y especialistas forenses tecnológicos que puedan aclarar los hechos ante la opinión pública, junto con las autoridades electorales.

Desde luego, para su implementación es indispensable que el sistema realice la autenticación de los votantes para confirmar que quien se presenta a votar sea quien dice ser, a través de biometría dactilar, facial y prueba de vida; así como protocolos criptográficos que aseguren la separación de los datos del votante y del voto emitido, ya que se debe mantener la secrecía del voto, el cual no debe quedar relacionado con los datos de quien lo emitió.

Ya que se debe asegurar la precisión del proceso, se tiene que cifrar la transacción para evitar que pueda ser alterada y para contribuir a la transparencia en el conteo y los resultados de la votación[6], aunque existen plataformas desarrolladas para llevar a cabo este tipo de procesos que cumplen con las garantías electorales de mantener la privacidad y el anonimato.

Cabe destacar que la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU., país que en 2016 posibilitó que 80 millones de personas votaran electrónicamente, realizó en 2020 un estudio para evaluar el riesgo cibernético de la infraestructura electoral, encontraron varios problemas con el sistema de votación electrónica de ese país que deben tenerse en cuenta.

Concluyeron que, si bien sus sistemas electorales integran infraestructuras y controles de seguridad, todos son potencialmente vulnerables a los ataques cibernéticos sofisticados, y aunque el riesgo es bajo, se deben tener planes de control y respuesta a incidentes porque las campañas de desinformación, en conjunto con los ataques cibernéticos, pueden entorpecer los procesos electorales y debilitar la confianza del público en los resultados de las elecciones[7].

Como se mencionó con anterioridad, en México se están implementado sistemas para votaciones electrónicas, por lo que se está a tiempo de aprender de las experiencias de otros países para ofrecer a los ciudadanos confiabilidad y certeza en la utilización de herramientas digitales para la votación, asegurando que el voto sea libre, secreto, individual, personal e intransferible[8].

Para ello, es imprescindible prevenir todo tipo de vulnerabilidades, tanto en el proceso como en los equipos de las casillas en donde se lleva a cabo la votación adoptando las mejores prácticas, implementación de controles, planes de contingencia, y auditorías previas a los sistemas para verificar su buen funcionamiento. Cabe mencionar que estas herramientas existen y se pueden conocer en foros como Infosecurity Mexico. Vale la pena actualizarse.

[6] https://bit.ly/42YAuiM
[7] https://bit.ly/42Nuzxd
[8] https://bit.ly/2F8kNdk