

Ponencia para el XXXVII Congreso Internacional de Estudios Electorales:

Soberanía digital y seguridad nacional: la nulidad electoral por intervención extranjera y la EIVE 2026-2036 ante los desafíos geopolíticos del proceso electoral mexicano 2026-2027

Obed Joao da Silva Botello¹

Licenciatura en Ciencia Política, Universidad Autónoma Metropolitana, Unidad Iztapalapa

Resumen:

La reforma constitucional publicada el 2 de junio de 2026 incorporó al artículo 41, base VI, inciso d), una causal expresa de nulidad electoral cuando se acrediten actos de intervención o injerencia extranjera que influyan en los resultados. Este cambio se inserta en una trayectoria normativa iniciada con la adición de 2025 al artículo 40 constitucional, que rechaza expresamente injerencias extranjeras en elecciones, y coincide con la institucionalización de la Estrategia Institucional de Voto Electrónico 2026-2036 (EIVE).

El presente trabajo analiza la relación entre soberanía nacional, integridad electoral, seguridad democrática e infraestructura digital del voto. La pregunta central es cómo debe responder el Estado mexicano ante riesgos de intervención extranjera sin transformar la nulidad electoral en una causal abstracta capaz de incentivar una judicialización excesiva de los resultados. Mediante un análisis jurídico-político con lectura geopolítica, se examinan el marco constitucional, el proyecto legislativo que dio origen a la reforma, la agenda pendiente de legislación secundaria y los riesgos tecnológicos identificados por el Instituto Nacional Electoral y por la literatura comparada sobre voto en línea. Se sostiene que la nueva causal puede fortalecer la defensa de la soberanía electoral siempre que su aplicación preserve exigencias de prueba objetiva y material, determinancia y trazabilidad.

Paralelamente, la EIVE puede ser entendida como una infraestructura institucional de resiliencia democrática, porque articula ciberseguridad, auditoría, continuidad operativa,

¹ Obed João da Silva Botello. Estudiante de Ciencia Política en la Universidad Autónoma Metropolitana (UAM), de Administración Pública en la Universidad Nacional Autónoma de México (UNAM) y de Ciencias de la Computación en Goldsmiths, University of London. Actualmente se desempeña como Asesor Operativo de Consejera Electoral en el Instituto Nacional Electoral (INE). Cuenta con experiencia en investigación política, análisis legislativo, procesos electorales y análisis multidisciplinario desde perspectivas política, administrativa y tecnológica. Correo: obedbotello333@gmail.com

verificabilidad y confianza pública. La conclusión principal es que la defensa contemporánea de la soberanía electoral exige integrar derecho, capacidades técnicas y análisis estratégico, evitando tanto la subestimación de amenazas externas como la expansión indeterminada del litigio poselectoral.

Keywords: *soberanía electoral; intervención extranjera; nulidad electoral; voto electrónico; EIVE; ciberseguridad; integridad electoral.*

Introducción:

La organización de elecciones dejó de ser un asunto circunscrito a la logística electoral. La digitalización de registros, mecanismos de identificación, sistemas de resultados, comunicaciones institucionales y modalidades de sufragio remoto ha ampliado la superficie sobre la que puede disputarse la integridad de un proceso electoral. En ese escenario, la soberanía electoral no depende únicamente de impedir financiamiento ilícito o intervenciones diplomáticas abiertas; también requiere capacidades para identificar operaciones de influencia, ataques informáticos, campañas de desinformación y otras formas de injerencia que pueden afectar la confianza pública aun cuando no modifiquen directamente una boleta. El problema es, por tanto, simultáneamente jurídico, político, tecnológico y estratégico.

En México, esta discusión adquirió una nueva dimensión constitucional. El artículo 40 fue reformado en 2025 para establecer que el pueblo mexicano no aceptará intervenciones, intromisiones o actos desde el extranjero lesivos de la integridad, independencia y soberanía de la Nación, incluyendo expresamente las injerencias en elecciones (Constitución Política de los Estados Unidos Mexicanos (CPEUM), 2026, art. 40). Un año después, el 2 de junio de 2026, se publicó en el Diario Oficial de la Federación (DOF) la adición del inciso d) a la base VI del artículo 41 constitucional, según la cual podrá declararse la nulidad cuando se acrediten actos de intervención o injerencia extranjera que influyan en los resultados electorales (DOF, 2026). La reforma no opera en el vacío: el propio artículo 41 conserva la exigencia de que las violaciones se acrediten de manera objetiva y material y mantiene la lógica de determinancia propia del sistema de nulidades (CPEUM, 2026, art. 41).

El cambio constitucional coincide con la aprobación del Acuerdo INE/CG471/2026 y de la Estrategia Institucional de Voto Electrónico con horizonte 2026-2036. La EIVE reconoce que la expansión del voto electrónico debe ser gradual y acompañarse de mecanismos de seguridad,

auditoría, verificabilidad, continuidad y construcción de confianza. Más aún, el documento dedica un apartado específico a los riesgos de posibles intrusiones extranjeras en sistemas electorales y a las recomendaciones internacionales para enfrentarlas (Instituto Nacional Electoral (INE), 2026, pp. 74-76). Esta coincidencia temporal permite formular una pregunta de investigación que trasciende el análisis técnico del voto electrónico: ¿cómo debe responder el Estado mexicano ante la posibilidad de intervención extranjera en elecciones sin producir una judicialización excesiva del resultado electoral ni debilitar la confianza en la autoridad electoral?

La hipótesis de este trabajo es que la nueva causal de nulidad puede fortalecer la defensa jurídica de la soberanía electoral si se interpreta de manera restrictiva, probatoria y verificable, y si se acompaña de reglas secundarias capaces de distinguir entre influencia política legítima, circulación transnacional de información y actos de injerencia materialmente relevantes. Al mismo tiempo, la EIVE debe leerse como una infraestructura crítica democrática: no sustituye la justicia electoral ni elimina el conflicto político, pero incrementa la capacidad del Estado para prevenir, detectar, auditar y explicar incidentes que puedan afectar la integridad del voto. La soberanía electoral, en consecuencia, se vuelve una relación entre norma, capacidad institucional y resiliencia tecnológica.

El texto se organiza en seis apartados. Primero se desarrolla un marco conceptual sobre soberanía, poder e integridad electoral. Segundo se examina la evolución constitucional mexicana de 2025 a 2026 y la agenda legislativa pendiente. Tercero se analiza la interferencia extranjera como problema de atribución, prueba y determinancia. Cuarto se estudia la dimensión geopolítica y las formas contemporáneas de influencia y presión. Quinto se analiza la EIVE 2026-2036 y la literatura comparada sobre voto en línea. Finalmente se propone un marco de articulación entre derecho electoral, seguridad nacional e infraestructura digital para el proceso electoral 2026-2027.

Metodología y alcance:

El trabajo utiliza una estrategia de análisis documental y jurídico-político. La base normativa está integrada por la Constitución vigente, el decreto publicado en el DOF el 2 de junio de 2026 y el proyecto de dictamen de la Comisión de Puntos Constitucionales que antecedió a la reforma. La dimensión institucional se estudia a partir del Acuerdo INE/CG471/2026 y de la EIVE 2026-2036. Para la dimensión comparada se emplean los trabajos de International IDEA sobre voto en línea y los materiales de ACE Project y de López Montiel sobre oportunidades, riesgos y

desafíos del voto electrónico. La lectura geopolítica se apoya en autores clásicos y contemporáneos de relaciones internacionales y poder, particularmente Morgenthau, Deutsch, Nye, Kagan, Kent y Baños.

El alcance es deliberadamente preventivo y analítico. No se pretende demostrar la existencia de una operación extranjera concreta sobre el proceso electoral mexicano de 2026-2027. Tampoco se equipara automáticamente la crítica internacional, la información proveniente del exterior, la actividad periodística o la interacción transnacional con una forma de injerencia jurídicamente sancionable. El objetivo es identificar las condiciones conceptuales y probatorias que permitirían distinguir entre fenómenos de influencia propios de una sociedad abierta y actos externos capaces de comprometer la autenticidad de una elección. Esta distinción es indispensable para evitar que el lenguaje de seguridad nacional se convierta, por sí mismo, en evidencia de una violación electoral.

Soberanía electoral, poder e integridad democrática:

La soberanía electoral puede entenderse como la capacidad de una comunidad política para renovar sus poderes mediante procedimientos cuya decisión final dependa de la ciudadanía y no de actores externos. Esta formulación combina dos dimensiones. La primera es normativa: la soberanía reside en el pueblo y las elecciones constituyen uno de los mecanismos mediante los cuales esa soberanía se ejerce. La segunda es estratégica: para que la decisión popular sea efectiva, el Estado debe disponer de instituciones capaces de proteger el proceso frente a presiones que busquen alterar la formación, expresión o cómputo de la voluntad política.

Desde la tradición realista, Morgenthau (1986) concibe la política internacional como una disputa por el poder en la que los Estados buscan preservar sus intereses en un sistema competitivo. Aunque su formulación clásica antecede por décadas a la digitalización electoral, resulta útil para evitar una lectura ingenua del entorno internacional: la existencia de normas no elimina las asimetrías de poder ni los incentivos de los actores para influir sobre otros Estados. Deutsch (1988), por su parte, permite observar que el poder no se reduce a la coerción militar; también involucra procesos de control, comunicación, información y capacidad de decisión. En contextos electorales digitalizados, esta ampliación conceptual es fundamental, porque una intervención relevante puede dirigirse a la información, a la percepción de legitimidad o a la infraestructura que sostiene el proceso.

Nye (2008) distingue formas de poder asociadas con coerción, incentivos y atracción. Esta perspectiva ayuda a separar la influencia internacional ordinaria de la injerencia que pretende sustituir o distorsionar la decisión política interna. Las democracias están expuestas de forma permanente a discursos, ideas, medios, campañas y referentes extranjeros; prohibir esa circulación sería incompatible con una sociedad plural. El problema jurídico comienza cuando un actor externo despliega recursos, capacidades o acciones encubiertas con la finalidad de alterar condiciones de competencia, afectar sistemas electorales o producir efectos determinantes sobre el resultado. La clave no es la extranjería de una voz, sino la naturaleza, intensidad, atribución y efecto de la conducta.

Kagan (2003) subraya que los Estados pueden desarrollar culturas estratégicas distintas respecto del uso del poder y de la confianza depositada en reglas e instituciones. Esta idea es relevante para México porque la evaluación de riesgos electorales no ocurre en un espacio abstracto, sino dentro de una relación asimétrica con potencias que disponen de capacidades económicas, tecnológicas, mediáticas y de inteligencia significativamente superiores. Sin embargo, reconocer una asimetría no autoriza a presumir una injerencia. En términos democráticos, el desafío consiste precisamente en construir capacidades de prevención y atribución sin sustituir la evidencia por sospechas geopolíticas.

La integridad electoral opera como puente entre soberanía y administración electoral. No basta con que la elección sea formalmente convocada por autoridades nacionales; también debe ser auténtica, libre, verificable y susceptible de escrutinio público. Por ello, la protección de la soberanía electoral debe concebirse como un sistema de capas: reglas constitucionales, controles de financiamiento, fiscalización, seguridad informática, auditorías, observación, mecanismos de impugnación y comunicación pública. La fortaleza del sistema depende menos de una sola barrera que de la capacidad de todas ellas para producir evidencia confiable y explicaciones comprensibles ante incidentes.

Del artículo 40 al artículo 41, constitucionalización de la injerencia extranjera:

La reforma de 2025 al artículo 40 marcó un cambio relevante en el lenguaje constitucional mexicano. El texto vigente dispone que el pueblo de México no aceptará intervenciones, intromisiones o actos desde el extranjero que sean lesivos de la integridad, independencia y soberanía de la Nación, y menciona expresamente las injerencias en elecciones (CPEUM, 2026,

art. 40). La incorporación de esta cláusula elevó la defensa frente a la injerencia electoral al nivel de principio constitucional de soberanía, pero todavía no definía por sí misma una consecuencia específica dentro del sistema de nulidades.

Ese vacío operativo fue el centro del proyecto de dictamen que antecedió a la reforma de 2026. La Comisión de Puntos Constitucionales sostuvo que las formas contemporáneas de injerencia pueden manifestarse mediante desinformación, manipulación digital, corrupción, espionaje, ciberataques, financiamiento y presiones diplomáticas, y consideró que la ausencia de una causal específica dificultaba una respuesta jurisdiccional directa (Comisión de Puntos Constitucionales, 2026, pp. 11-14). El argumento legislativo, por tanto, conectó la soberanía general del artículo 40 con una consecuencia electoral concreta en el artículo 41.

El decreto publicado el 2 de junio de 2026 adicionó el inciso d) a la base VI del artículo 41. La causal establece que podrán anularse elecciones cuando 'se acrediten actos de intervención o injerencia extranjera que influyan en los resultados electorales' (DOF, 2026). Su importancia radica en dos elementos. Primero, la Constitución ya no se limita a prohibir la injerencia, sino que la incorpora expresamente al sistema de nulidades. Segundo, la redacción utiliza un estándar de influencia sobre resultados, lo que obliga a desarrollar criterios de acreditación, atribución y determinancia compatibles con el resto del sistema constitucional.

La propia base VI señala que las violaciones deben acreditarse de manera objetiva y material y presume su determinancia, para las causales del sistema, cuando la diferencia entre primero y segundo lugar es menor al cinco por ciento (CPEUM, 2026, art. 41). Esta arquitectura resulta decisiva: impide leer el inciso d) como una cláusula puramente política o retórica. La nulidad de una elección es una medida extrema porque invalida la expresión agregada de la ciudadanía. En consecuencia, la interpretación de una causal nueva debe ser rigurosa para que el remedio no produzca un daño democrático mayor que la conducta que pretende sancionar.

El decreto también ordenó armonizar el marco normativo y revisar disposiciones administrativas de las autoridades electorales (DOF, 2026). Sin embargo, el desarrollo secundario permanece como una tarea legislativa específica. El documento de temas legislativos para el primer periodo ordinario del tercer año de ejercicio de la LXVI Legislatura incluye, como punto 5, una 'Ley secundaria en materia de nulidad por intervención o injerencia extranjera' (Cámara de Diputados, 2026). Esto significa que el problema central de 2026 ya no es si existe la causal constitucional -pues está vigente-, sino cómo se definirá su operación procesal.

Esa legislación secundaria debería resolver al menos cinco cuestiones. La primera es la definición de intervención o injerencia extranjera. La segunda es el estándar de atribución: qué nivel de evidencia se requiere para vincular una acción con un actor extranjero estatal o no estatal. La tercera es el nexo causal entre la conducta y los resultados electorales. La cuarta es la determinancia, particularmente cuando el impacto sea informacional y no se traduzca en una alteración directa del cómputo. La quinta es el régimen probatorio y de coordinación entre autoridades electorales, administrativas, de seguridad y, en su caso, de inteligencia. Sin estas precisiones, la causal corre el riesgo de convertirse en un concepto jurídico demasiado abierto.

Interferencia extranjera, prueba y riesgo de judicialización:

La principal tensión de la reforma se encuentra entre protección y judicialización. Toda causal de nulidad persigue proteger la autenticidad electoral, pero también crea incentivos para que los actores derrotados trasladen la competencia política al terreno jurisdiccional. En las causales tradicionales, el sistema mexicano ha desarrollado umbrales, metodologías y criterios para evaluar gastos, recursos, cobertura y determinancia. En el caso de la injerencia extranjera, el reto es mayor porque las conductas pueden ser indirectas, transnacionales, digitales, opacas o ejecutadas por redes de actores cuya atribución resulte compleja.

La primera exigencia debe ser distinguir influencia de intervención. La política internacional produce influencia de manera cotidiana. Declaraciones de gobiernos, opiniones de líderes extranjeros, cobertura mediática, contenidos digitales, organizaciones transnacionales y diásporas participan legítimamente en la esfera pública. La injerencia jurídicamente relevante debería reservarse para conductas que incorporen elementos de intencionalidad, coordinación, ocultamiento, provisión de recursos, intrusión tecnológica o presión indebida y que tengan una relación demostrable con la competencia electoral. Sin esta distinción, prácticamente cualquier discusión internacional sobre una elección podría convertirse en materia de impugnación.

La segunda exigencia es la atribución. En ciberseguridad, identificar el origen técnico de una intrusión no equivale necesariamente a demostrar quién la ordenó, financió o dirigió. El INE reconoce que los actores estatales pueden disponer de recursos financieros amplios, equipos especializados y capacidad para atacar componentes como registros de electores, sistemas de resultados o sistemas de voto electrónico (INE, 2026, pp. 74-75). Precisamente por esa sofisticación, la atribución debe construirse a partir de evidencia convergente y no de inferencias

políticas. Un tribunal electoral necesitaría elementos técnicos, contextuales y documentales suficientemente robustos para vincular la conducta con el actor y con la elección.

La tercera exigencia es demostrar el efecto. La redacción constitucional exige que los actos 'influyan en los resultados electorales'. El concepto de influencia puede abarcar desde una alteración directa de datos hasta efectos sobre preferencias ciudadanas, participación, confianza o aceptación de resultados. Pero no todos esos efectos pueden medirse con la misma precisión. Por ello, la legislación secundaria debe evitar una equivalencia automática entre exposición a desinformación y determinancia electoral. La existencia de una campaña de influencia puede ser grave y sancionable sin que necesariamente permita demostrar que cambió el resultado de una elección concreta.

La cuarta exigencia es preservar la proporcionalidad. La nulidad debe funcionar como última respuesta cuando la violación sea grave y determinante. Si la evidencia permite identificar un ataque o una campaña pero el sistema electoral demuestra que el voto, el cómputo y la cadena de resultados conservaron su integridad, la respuesta puede requerir sanciones, investigación o medidas de seguridad sin llegar necesariamente a invalidar la elección. Esta separación entre incidente de seguridad y nulidad electoral es esencial para impedir que el propio ataque logre su objetivo político mediante la erosión de la confianza pública.

Finalmente, existe un problema de comunicación. Una elección puede ser técnicamente segura y, al mismo tiempo, socialmente percibirse como vulnerable. International IDEA advierte que las evaluaciones de riesgo del voto en línea no pueden limitarse a variables técnicas, sino que deben funcionar también como procesos sociales de construcción de confianza (Barrat i Esteve, 2025, pp. 32-33). La misma lógica es aplicable a la injerencia extranjera: la autoridad debe ser capaz de explicar qué ocurrió, qué evidencia existe, qué parte del sistema fue afectada y por qué el incidente compromete o no el resultado. En ausencia de comunicación verificable, la sospecha puede ser tan destabilizadora como el ataque.

Geopolítica de la intervención electoral en la era digital:

La incorporación de una causal de nulidad por intervención extranjera refleja una transformación del entorno de seguridad. Las fronteras entre política exterior, comunicación, tecnología y procesos electorales son cada vez más porosas. CEPAL ha caracterizado el escenario regional como una nueva era geopolítica marcada por creciente rivalidad y por la necesidad de que

América Latina fortalezca su gobernanza, movilice capacidades estratégicas y amplíe su margen de acción y negociación (CEPAL, 2026). Para el ámbito electoral, esto significa que la autonomía política también depende de capacidades tecnológicas y de coordinación que antes podían considerarse periféricas.

Kent (1949) definió la inteligencia estratégica como conocimiento útil para orientar decisiones vinculadas con la seguridad y los intereses nacionales. Trasladada al terreno electoral, esta idea no implica militarizar la administración de elecciones, sino reconocer la necesidad de anticipar riesgos, distinguir señales de ruido y construir escenarios. Una autoridad electoral no es un servicio de inteligencia, pero puede beneficiarse de mecanismos institucionales de intercambio de información que permitan evaluar amenazas sobre infraestructura crítica sin comprometer su independencia constitucional.

La digitalización modifica además la escala de las operaciones de influencia. Baños (2020) pone el acento en el papel de la información, la comunicación y las técnicas de persuasión en la formación de percepciones colectivas, mientras que su análisis de los instrumentos contemporáneos del poder destaca la relevancia creciente de la tecnología y el conocimiento (Baños, 2024). Estas obras deben utilizarse con cautela y como marcos interpretativos, no como evidencia de una operación concreta. Su utilidad reside en recordar que la competencia estratégica contemporánea puede buscar efectos cognitivos y políticos sin recurrir a una intervención territorial abierta.

En este contexto, la noción de “*guerra híbrida*” suele emplearse para describir combinaciones de instrumentos convencionales y no convencionales, estatales y no estatales, visibles y encubiertos. Para un análisis electoral riguroso, sin embargo, el término no debe convertirse en una categoría totalizante. Si todo desacuerdo internacional o toda campaña digital se define como guerra híbrida, la categoría pierde capacidad explicativa y se vuelve políticamente peligrosa. La utilidad analítica está en identificar mecanismos concretos: intrusión, suplantación, filtración de información, financiamiento oculto, manipulación coordinada o afectación de sistemas críticos.

La soberanía digital, por ello, no equivale a aislamiento informacional. Se refiere más bien a la capacidad institucional de un Estado para decidir sobre procesos críticos, proteger datos y sistemas, exigir estándares a proveedores, mantener competencias técnicas internas y conservar evidencia verificable de sus operaciones. International IDEA subraya que la propiedad y

supervisión efectiva del sistema por parte de los organismos electorales es un factor importante para el éxito del voto en línea, especialmente cuando intervienen proveedores externos (Barrat i Esteve, 2025, pp. 33-34). La dependencia tecnológica sin capacidad de auditoría puede convertirse en una vulnerabilidad estratégica, incluso cuando no exista una intervención maliciosa.

Desde esta perspectiva, el objetivo de una política de seguridad electoral no debe ser prometer invulnerabilidad. Ningún sistema digital complejo puede garantizar riesgo cero. El objetivo es construir resiliencia: reducir la probabilidad de intrusión, limitar el daño, detectar incidentes, mantener continuidad operativa, conservar evidencia y recuperar la confianza. Esa lógica es compatible tanto con la seguridad nacional como con los principios democráticos porque desplaza el énfasis de la opacidad hacia la verificabilidad.

La EIVE 2026-2036 como infraestructura de resiliencia electoral:

La Estrategia Institucional de Voto Electrónico 2026-2036 constituye el componente técnico central de esta ponencia. Su importancia no radica en sustituir el voto en papel, sino en ordenar una política de largo plazo para modalidades electrónicas bajo un enfoque gradual, cauteloso y sujeto a evaluación. La estrategia contempla voto presencial con urnas electrónicas, dispositivos electrónicos en módulos receptores de votación en sedes consulares, el Sistema de Voto Electrónico por Internet (SIVEI) para mexicanas y mexicanos residentes en el extranjero y una modalidad de voto anticipado por internet dirigida a personas con discapacidad imposibilitadas para acudir a su casilla y a sus personas cuidadoras (INE, 2026, pp. 46-63).

El valor institucional de estas modalidades es doble. Por una parte, amplían condiciones de accesibilidad y pueden reducir barreras para grupos específicos. Por otra, convierten componentes tecnológicos en piezas directamente vinculadas con la autenticidad del sufragio. Esta segunda dimensión obliga a analizarlos como infraestructura electoral crítica: su diseño, propiedad, auditoría, seguridad, continuidad y trazabilidad afectan no sólo la eficiencia administrativa, sino la legitimidad de la elección.

La EIVE reconoce expresamente riesgos asociados con secrecía, coacción en entornos remotos, suplantación de identidad, transparencia, integridad tecnológica, confianza ciudadana, brecha digital y verificabilidad (INE, 2026, pp. 84-90). Esta enumeración es relevante porque demuestra que la autoridad electoral no reduce el problema del voto electrónico a ciberseguridad.

La confianza en un sistema depende también de su comprensión, de la posibilidad de auditarlo y de que los actores políticos puedan ejercer una supervisión significativa.

En materia de amenazas externas, la estrategia adopta referencias internacionales y recomienda medidas como arquitectura de seguridad por capas, autenticación reforzada, auditorías y pruebas continuas, capacidad de recuperación, monitoreo permanente, mecanismos de verificabilidad, análisis de riesgos de ataques estatales y modelos de confianza cero (INE, 2026, pp. 74-76). Este conjunto de medidas aproxima la administración electoral a una lógica de resiliencia: asumir que la infraestructura puede ser atacada y diseñar el sistema para detectar, contener y recuperar.

International IDEA llega a conclusiones compatibles desde la experiencia comparada. El voto en línea exige evaluaciones de riesgo y factibilidad, un marco jurídico claro, apropiación institucional por parte del organismo electoral, escenarios de crisis, transparencia, auditorías y pruebas oportunas (Barrat i Esteve, 2025, pp. 29-50). En particular, las auditorías no son sólo controles técnicos: contribuyen a construir confianza, porque compensan el efecto de 'caja negra' inherente a tecnologías que la mayoría de los votantes no puede verificar directamente (Barrat i Esteve, 2025, pp. 45-47).

ACE Project coincide en que el voto electrónico ofrece oportunidades de accesibilidad, participación remota y rapidez de resultados, pero también identifica riesgos como intervención no autorizada de terceros, dificultad para detectar fallas y problemas para garantizar identidad, unicidad y secrecía en contextos remotos (ACE Project, s. f.). En México, López Montiel (2014) ya advertía que la incorporación de tecnología electoral debía analizarse junto con condiciones legales, presupuestales y de legitimidad, y no únicamente como una cuestión de modernización técnica.

La experiencia acumulada por el INE también muestra que la resiliencia debe incluir fallas ordinarias. Los anexos de la EIVE documentan incidentes asociados con pantallas congeladas, módulos de impresión, suministro eléctrico, tarjetas de configuración y sustitución de equipos, así como planes de continuidad y soporte técnico. En Coahuila, durante la prueba piloto 2025-2026, se reportaron incidentes que fueron solventados y de los que se derivó la necesidad de reforzar capacitación, modelos operativos y contingencias (INE, 2026). Estos casos son relevantes porque recuerdan que una falla no es automáticamente un ciberataque y que la capacidad de distinguir entre error operativo e intervención maliciosa es parte de la seguridad electoral.

La auditoría del SIVEI constituye otro elemento central. La EIVE reporta revisiones técnicas orientadas a verificar funcionalidad, infraestructura, disponibilidad, cifrado y manejo de información. Desde el punto de vista de soberanía digital, la auditoría externa e independiente ayuda a producir evidencia que puede utilizarse tanto para prevenir riesgos como para responder a narrativas de fraude. Una política de voto electrónico madura necesita, por tanto, no sólo controles internos, sino mecanismos que permitan a terceros calificados evaluar la integridad del sistema dentro de límites compatibles con la seguridad de la información.

Aquí aparece una tensión inevitable entre transparencia y seguridad. Publicar todos los detalles técnicos puede facilitar ataques; ocultarlos en exceso puede erosionar la confianza. International IDEA analiza precisamente el caso mexicano y señala que el acceso a información sobre auditorías puede entrar en tensión con la necesidad de proteger datos cuya divulgación incrementaría vulnerabilidades (Barrat i Esteve, 2025, pp. 46-47). La EIVE reconoce la misma tensión (INE, 2026, p. 76). La respuesta no debe ser transparencia absoluta ni secreto total, sino modelos escalonados de acceso, auditoría independiente y publicación de resultados suficientes para permitir control democrático sin exponer superficies críticas.

Hacia un modelo integrado para el proceso electoral 2026-2027:

La reforma constitucional y la EIVE pueden integrarse en un mismo marco de política pública si se evita confundir sus funciones. La causal de nulidad pertenece al ámbito de la justicia electoral y opera después de que una conducta presuntamente ilícita ha afectado la elección. La EIVE pertenece al ámbito de organización y seguridad electoral y busca reducir vulnerabilidades antes y durante la votación. Una protege mediante consecuencias jurídicas; la otra mediante capacidades técnicas y procedimientos verificables. Su complementariedad es más sólida cuando cada instrumento conserva sus límites.

Para el proceso 2026-2027 puede proponerse un ciclo de cuatro momentos. El primero es prevención: evaluación de riesgos, pruebas, auditorías, capacitación, revisión de proveedores y protocolos de coordinación. El segundo es detección: monitoreo de infraestructura, registro de incidentes, preservación de evidencia y mecanismos de escalamiento. El tercero es atribución y evaluación: análisis técnico y jurídico que distinga fallas, delitos comunes, desinformación, intervención externa y afectación real de resultados. El cuarto es respuesta pública y jurisdiccional:

continuidad operativa, comunicación, sanciones y, sólo cuando se satisfagan los estándares constitucionales, eventual nulidad.

Este ciclo exige también un modelo probatorio interdisciplinario. La justicia electoral no puede depender exclusivamente de peritajes informáticos, pero tampoco puede resolver incidentes digitales complejos sólo con categorías jurídicas tradicionales. Sería recomendable que la legislación secundaria estableciera reglas para la conservación de registros técnicos, cadenas de custodia digital, peritajes independientes, intercambio de información entre autoridades y protección de información sensible. La finalidad no es crear una excepción de seguridad nacional a la transparencia electoral, sino asegurar que la evidencia necesaria para resolver un litigio exista, sea íntegra y pueda ser controvertida por las partes.

Otro componente es la comunicación estratégica institucional. La autoridad electoral debe prepararse para escenarios en los que una narrativa de intervención se difunda antes de que exista evidencia concluyente. Una respuesta tardía, contradictoria o excesivamente técnica puede ampliar la incertidumbre. Por ello, los protocolos deberían distinguir entre información confirmada, hipótesis bajo investigación y rumores no sustentados. La credibilidad institucional se fortalece cuando la autoridad reconoce límites de conocimiento y explica el proceso mediante el cual verificará un incidente.

También debe evitarse que la seguridad electoral se convierta en una política de exclusión. La expansión del voto electrónico puede reproducir desigualdades por acceso, habilidades digitales o disponibilidad de dispositivos. La propia EIVE identifica la brecha digital como riesgo (INE, 2026, pp. 87-90). International IDEA recomienda un enfoque contextual y gradual, señalando que ninguna solución es universal y que la adopción debe responder a necesidades locales, confianza social, marco jurídico y capacidad institucional (Barrat i Esteve, 2025, pp. 77-78). En consecuencia, la resiliencia electoral debe incorporar accesibilidad, alternativas de votación y mecanismos de asistencia.

Finalmente, México debe considerar la dimensión regional. La CEPAL (2026) insiste en que América Latina requiere fortalecer capacidades propias frente a una etapa de mayor competencia geopolítica. En materia electoral, la cooperación regional puede traducirse en intercambio de estándares de ciberseguridad, experiencias de auditoría, protocolos de respuesta a incidentes y mecanismos de aprendizaje entre organismos electorales. La soberanía no se debilita

por cooperar; puede fortalecerse cuando la cooperación reduce dependencias y amplía capacidades técnicas.

Conclusiones:

La reforma al artículo 41 constitucional representa un cambio sustantivo en la arquitectura mexicana de nulidades electorales. Desde junio de 2026, la intervención o injerencia extranjera dejó de ser únicamente un principio de rechazo asociado con la soberanía y pasó a constituir una causal expresa de nulidad cuando se acredite su influencia en los resultados. Esta innovación responde a un entorno en el que las amenazas a la integridad electoral pueden adoptar formas digitales, informacionales y transnacionales. Sin embargo, precisamente por la amplitud de esas formas, la eficacia de la reforma dependerá de que su desarrollo secundario reduzca ambigüedades y preserve estándares probatorios elevados.

El riesgo principal no es solamente subestimar una intervención externa. También lo es sobredimensionar cualquier influencia internacional hasta convertirla en causal de invalidez electoral. La protección de la soberanía exige distinguir entre circulación legítima de información, influencia política transnacional, campañas coordinadas, financiamiento indebido, intrusiones informáticas y actos efectivamente determinantes. La legislación secundaria deberá construir estas fronteras con precisión, porque una causal excesivamente abierta puede incentivar litigiosidad estratégica y trasladar la decisión electoral desde la ciudadanía hacia una disputa permanente sobre narrativas de injerencia.

La EIVE 2026-2036 ofrece un segundo componente de respuesta. Su aportación no consiste en hacer invulnerable la elección, sino en construir capacidades de resiliencia: evaluación de riesgos, seguridad por capas, autenticación, auditoría, verificabilidad, continuidad operativa, monitoreo y aprendizaje institucional. Estas capacidades son especialmente relevantes para modalidades de voto electrónico y extraterritorial, donde la infraestructura digital se vuelve parte directa de la cadena de confianza democrática.

La relación entre la nueva causal y la EIVE permite una conclusión más amplia. En la democracia digital, la soberanía electoral no puede protegerse únicamente con prohibiciones constitucionales ni únicamente con tecnología. El derecho necesita evidencia técnica; la tecnología necesita reglas, controles y legitimidad; la seguridad necesita límites democráticos; y la justicia

electoral necesita criterios capaces de diferenciar una amenaza real de una controversia política. La defensa de la elección es, por tanto, una tarea interinstitucional y multidimensional.

De cara al proceso electoral 2026-2027, la mejor respuesta institucional no es partir de la presunción de que existirá una intervención extranjera, sino construir un sistema preparado para identificarla si ocurre y demostrar, con evidencia verificable, qué efectos produjo. Sólo así la nueva causal podrá operar como salvaguarda de la soberanía y no como fuente adicional de incertidumbre. La legitimidad democrática dependerá tanto de la capacidad de resistir ataques como de la capacidad de explicar públicamente por qué el resultado electoral merece confianza.

Referencias:

- ACE Project. (s. f.). *Oportunidades, riesgos y desafíos del voto electrónico*. ACE Electoral Knowledge Network.
- Baños, P. (2020). *El dominio mental: La geopolítica de la mente*. Ariel.
- Baños, P. (2024). *El dominio mundial: Elementos del poder y claves geopolíticas*. Ariel.
- Barrat i Esteve, J. (2025). *Online voting: Current and future practices*. International IDEA. <https://doi.org/10.31752/idea.2025.69>
- Cámara de Diputados. (2026). Temas legislativos por abordarse en el primer periodo ordinario del tercer año de ejercicio de la LXVI Legislatura.
- Comisión de Puntos Constitucionales. (2026). *Proyecto de dictamen a la iniciativa con proyecto de decreto por el que se adiciona un inciso a la base VI del artículo 41 de la Constitución Política de los Estados Unidos Mexicanos, para introducir una nueva causal de nulidad de elecciones por intervención extranjera*.
- Comisión Económica para América Latina y el Caribe. (2026). *Rupturas y oportunidades: Propuestas para que América Latina y el Caribe prospere en la nueva era geopolítica*.
- Constitución Política de los Estados Unidos Mexicanos. (2026). Cámara de Diputados del H. Congreso de la Unión. Últimas reformas publicadas en el Diario Oficial de la Federación el 2 de junio de 2026.
- Deutsch, K. W. (1988). *The analysis of international relations*. Prentice Hall.
- Diario Oficial de la Federación. (2026, 2 de junio). Decreto por el que se adiciona un inciso a la base VI del artículo 41 de la Constitución Política de los Estados Unidos

Mexicanos, para introducir una nueva causal de nulidad de elecciones por intervención extranjera.

- Instituto Nacional Electoral. (2026). *Acuerdo INE/CG471/2026 por el que se aprueba la Estrategia Institucional de Voto Electrónico con horizonte de corto, mediano y largo plazo 2026-2036*.
- Kagan, R. (2003). *Poder y debilidad: Estados Unidos y Europa en el nuevo orden mundial*. Taurus.
- Kent, S. (1949). *Inteligencia estratégica para la política mundial norteamericana*.
- López Montiel, G. (2014). *Los desafíos del voto electrónico en México*.
- Morgenthau, H. J. (1986). *Política entre las naciones: La lucha por el poder y la paz* Grupo Editor Latinoamericano.
- Nye, J. S., Jr. (2008). *The powers to lead*. Oxford University Press.