



NATIONAL
DEMOCRATIC
INSTITUTE

**Tecnología y principios electorales:
Panorama de proveedores
2022**

Índice

Introducción.....	1
Tecnología Proporcionada por Los Proveedores	2
Registro y verificación de votantes	2
Registro y creación de una lista de votantes.....	2
Gestión y almacenamiento de datos del censo electoral.....	3
Verificación de los votantes.....	3
Procesos de votación y recuento	3
Transmisión, tabulación y anuncio de resultados	4
Servicios básicos de tecnología de la información y ciberseguridad	5
Otros usos de la tecnología en las elecciones	5
Mercado tecnológico electoral: Panorama de los proveedores	5
Principios de integridad en la tecnología electoral	7
Principios en la práctica: Regulación de proveedores, requisitos y políticas internas	14
<i>Normativa gubernamental</i>	14
<i>Mandatos y normas de contratación</i>	14
<i>Coordinación de proveedores</i>	15
<i>Códigos de conducta y políticas corporativas voluntarias</i>	15
Conclusión.....	15

Introducción

La introducción de tecnologías electrónicas en las elecciones puede mejorar significativamente elementos de los procesos electorales. Sin embargo, la adopción de tecnologías electrónicas puede presentar riesgos para la integridad electoral y la confianza de los ciudadanos. Las decisiones relativas a la adopción de tales tecnologías electorales no son simplemente cuestiones "técnicas", sino que a menudo deben ser objeto de debates públicos abiertos e inclusivos sobre políticas. Una vez concluidas adecuadamente las deliberaciones políticas inclusivas, seguir adelante suele ser responsabilidad de los funcionarios electorales, aunque en muchos países los organismos internacionales de asistencia y las organizaciones de ayuda desempeñan papeles importantes que pueden influir en la adopción de la tecnología.

Durante décadas, los organismos electorales (OE) han introducido la tecnología en los procesos electorales en un intento de resolver los problemas de acceso, desigualdad, ineficacia y transparencia. Sin embargo, cuando los OE adoptan diversas tecnologías (a menudo subcontratando a proveedores externos diversos equipos y programas informáticos y/o servicios conexos), siguen siendo aplicables los principios universales de las elecciones democráticas y las mejores prácticas que los sustentan. Los OE no sólo tienen que considerar cómo pueden mantenerse los principios democráticos y las mejores prácticas a medida que se introducen las tecnologías, sino que los proveedores deben garantizar que estos principios se cumplen en el diseño y la implementación de las herramientas. Otras partes interesadas, incluidos los partidos políticos y los observadores ciudadanos e internacionales que supervisan el proceso, así como los donantes y los proveedores de asistencia técnica que apoyan el proceso, también deben promover estos principios a través de su trabajo.

Este documento pretende ayudar a los profesionales que asesoran, implementan o supervisan la aplicación de la tecnología en un proceso electoral, ayudándoles a comprender mejor el espacio de los proveedores y el papel potencial que éstos pueden desempeñar en la promoción y adopción de principios electorales sólidos. El documento examina los tipos de tecnologías que se utilizan habitualmente en los procesos electorales oficiales y ofrece una visión general del "mercado" de la tecnología electoral. Además, el documento repasa los principios electorales clave y las mejores prácticas¹ que los proveedores -y quienes los gestionan- deben tener en cuenta a la hora de identificar, diseñar e implementar soluciones tecnológicas, así como las posibles vías para promover esos principios en el espacio de los proveedores.

Para los fines de este documento, el término "proveedor" se aplica a cualquier organización externa, ya sea una empresa privada, pública o estatal o una entidad estatal externa, que

¹ Este documento se basa en los principios establecidos en los Principios Generales y Directrices relacionados con las TIC y las Elecciones por el Grupo de Trabajo e-TIC de la comunidad de práctica de la Declaración de Principios para la Observación Internacional.

proporcione servicios y bienes de tecnología electoral a un OE, ya sea a un costo o de forma gratuita a través de la financiación de la ayuda internacional o la "donación" del proveedor. Este documento se centra en la tecnología específica para los procesos electorales, más que en el hardware o software de uso general y disponible en el mercado utilizado por los OE. Este documento no tiene en cuenta la tecnología utilizada por otros actores electorales, incluidos los partidos políticos o los observadores electorales, ya que estas tecnologías no se utilizan en los procesos electorales oficiales y no están sujetas a las mismas obligaciones en virtud de la legislación nacional o los compromisos internacionales formales.

1. Tecnología Proporcionada por Los Proveedores

Las tecnologías proporcionadas por los proveedores ayudan en procesos que van desde la planificación preelectoral y la gestión del personal hasta el registro de los votantes, y desde la emisión de los votos y la tabulación y el anuncio de los resultados hasta la auditoría. Cada país utiliza la tecnología de una manera única, ya que los problemas que las tecnologías tratan de resolver - así como las leyes que rigen el proceso y el contexto tecnológico - varían significativamente de un país a otro. Las siguientes secciones describen aspectos de las elecciones actuales en los que las tecnologías se emplean habitualmente (aunque ciertamente no de forma universal).²

Registro y verificación de votantes

Las tecnologías se utilizan ampliamente para apoyar el registro de votantes, desde la recopilación y verificación de la información de los votantes hasta la gestión de una base de datos de votantes y la verificación de los votantes en los centros de votación. Esto puede incluir lo siguiente.

Registro y creación de una lista de votantes

Se pueden utilizar tecnologías para recopilar información personal de los votantes potenciales, ya sea a través de funcionarios de registro móviles, oficinas fijas o sitios web oficiales. Como mínimo, la información de los votantes, como el nombre, la edad y la dirección, puede recopilarse y digitalizarse a través de la entrada/grabación directa (como llenar un formulario electrónico en una tableta o computadora) o tecnologías de escaneo óptico que digitalizan formularios en papel. Algunos países recogen identificadores personales adicionales de los ciudadanos, como firmas o números de documentos de identidad oficiales, o datos biométricos como fotografías, huellas dactilares y/o escáneres del iris.

Dependiendo del marco legal y administrativo, algunos países crean su lista de votantes a partir de datos (informativos y/o biométricos) recogidos para un registro civil. En tales casos, las tecnologías utilizadas para el registro civil se considerarían tecnologías electorales.

² Para más detalles sobre estas tecnologías específicas, consulte en IFES y NDI , ["Implementación y supervisión de las tecnologías de votación y recuento electrónicos" \(en inglés\)](#) (2013); y en NDI ["Monitoreo de las tecnologías electrónicas en los procesos electorales" \(en inglés\)](#) (2007).

Gestión y almacenamiento de datos del censo electoral

Los organismos electorales suelen utilizar tecnologías, incluido software especializado de gestión de datos y bases de datos, para compilar, verificar y gestionar una lista de votantes. El software puede comprobar la existencia de duplicaciones y errores y, en algunos casos, realizar comprobaciones cruzadas con otras fuentes oficiales (como un registro civil) para verificar los documentos de identidad o la elegibilidad de los votantes. La tecnología también se utiliza para almacenar la base de datos de la lista de votantes en una plataforma segura, ya sea remota (basada en la nube) o en un servidor local. En algunos países, las tecnologías pueden utilizarse para hacer que la lista de votantes sea más accesible y transparente, incluidas herramientas de búsqueda en la web o plataformas de medios sociales que permiten a los votantes comprobar su registro, o interfaces de programación de aplicaciones (API) que proporcionan a socios seleccionados (como partidos políticos, medios de comunicación, organizaciones de la sociedad civil y otros) acceso a datos no confidenciales de la lista de votantes.

Verificación de los votantes

Algunos países utilizan tecnología para verificar la identidad de los votantes en los centros de votación. Esto puede incluir tabletas o computadoras y programas informáticos utilizados para registrar a un votante. En algunos países, esto incluye la verificación electrónica de las identificaciones de los votantes o de datos biométricos como fotos o huellas dactilares. En los sistemas de voto por correo, las tecnologías se utilizan habitualmente para clasificar, procesar y/o verificar los sobres de votación (mediante escáner óptico o, con menor frecuencia, software de verificación de firmas).

Procesos de votación y recuento

Algunos países utilizan la tecnología para distribuir las papeletas y/o emitir y registrar los votos, ya sea en un centro de votación o a distancia a través de dispositivos móviles, Internet o el servicio postal. Para la votación presencial en algunos países, los votantes (o un subconjunto de votantes, como las personas con discapacidad que no pueden marcar una papeleta de papel) pueden utilizar un **dispositivo de marcado de papeletas (DMO)**, en el que el votante utiliza una pantalla táctil u otra tecnología para ver la papeleta e indicar su elección. Una vez indicada la opción del votante, la máquina imprime una papeleta marcada, que se deposita en una urna. Algunos países utilizan **escáneres ópticos** para contar los votos marcados en papeletas, ya sean marcadas a mano en un colegio electoral, impresas/marcadas por una DMO o enviadas por correo por un votante. Otros países utilizan **dispositivos electrónicos de registro directo (DRE, por sus siglas en inglés)**, en los que los votantes utilizan una pantalla táctil u otra tecnología para indicar su elección y enviar electrónicamente su voto. (De acuerdo con los principios de integridad electoral, los DRE deben incluir un rastro de papel auditable y verificado por el votante).

En la última década, han surgido nuevas tecnologías para apoyar el voto a distancia a través de herramientas móviles y/o en línea. Algunas tecnologías de votación en línea son híbridas, en las que la papeleta se entrega por Internet, se marca electrónicamente, se

imprime y se devuelve por correo u otro método.³ En comparación, los sistemas enteramente en línea, en los que los votantes reciben, marcan y envían una papeleta a través de Internet, no son de uso generalizado, y las aplicaciones, métodos y medidas de seguridad específicos varían. Algunos sistemas, como el voto por Internet que se lleva a cabo en Estonia, se basan en un proceso "de extremo a extremo" que vincula el registro de votantes/civiles (a menudo utilizando datos biométricos), la verificación de los votantes y la votación en línea con el objetivo de mitigar el fraude electoral. Algunos sistemas utilizan diferentes formas de medidas de seguridad mejoradas, como el cifrado o los libros de contabilidad distribuidos (como blockchain), para mitigar el riesgo de piratería informática. A pesar de estas medidas, los expertos en seguridad del voto siguen siendo escépticos en cuanto a que las tecnologías actuales puedan garantizar la transparencia, el secreto del voto y las medidas de seguridad y rendición de cuentas necesarias para celebrar elecciones legalmente vinculantes que mantengan la confianza pública.⁴

Transmisión, tabulación y anuncio de resultados

También se utilizan tecnologías para transmitir, tabular y anunciar los resultados electorales. Esto puede incluir la transmisión de los resultados desde los centros de votación a centros de tabulación centrales o bases de datos, utilizando Datos de Servicio Suplementario No Estructurados (USSD, por sus siglas en inglés), mensajes de texto enviados a través de sistemas de mensajes cortos (SMS), o sistemas basados en Internet. Estos sistemas incluyen a veces medidas de seguridad adicionales, como la encriptación, para evitar la piratería informática. Algunos países utilizan esta tecnología para informar rápidamente de los resultados preliminares (mientras que los resultados legalmente oficiales se transmiten en formularios en papel o por otros canales), mientras que otros confían en la tecnología para transmitir los resultados oficiales.

Una vez recibidos los votos oficiales, puede utilizarse tecnología (como programas informáticos especiales y bases de datos seguras) para contabilizar los resultados, confirmar los candidatos ganadores y/o asignar los puestos de acuerdo con el marco jurídico y el sistema electoral.

En muchos países, las tecnologías se utilizan a menudo para mostrar y comunicar los resultados. Esto puede incluir sitios web oficiales que muestran los totales agregados de votos y los ganadores de las contiendas. En muchos casos, estos sitios web están separados del sitio principal de un organismo de gestión electoral y son diseñados, alojados y mantenidos por un proveedor externo. En algunas elecciones, los resultados agregados o

³ Tenga en cuenta que este enfoque híbrido (a veces denominado "entrega remota del voto") se utiliza a menudo cuando el marco legal no permite la votación en línea (recibir, marcar y enviar un voto a través de Internet). Algunos países utilizan el voto a distancia para igualar el acceso al voto de determinados grupos de votantes, como los votantes en el extranjero o los militares, o los votantes con discapacidades que no pueden votar en persona.

⁴ Consulte <https://www.csail.mit.edu/news/mit-experts-no-dont-use-blockchain-vote>, <https://www.aaas.org/programs/epi-center/internet-online-voting>, y <https://verifiedvoting.org/the-myth-of-secure-blockchain-voting/>.

desglosados pueden ponerse a disposición de un público selecto (como los medios de comunicación) o del público a través de una API u [otros medios de datos abiertos](#).⁵

Servicios básicos de tecnología de la información y ciberseguridad

Es cada vez más frecuente que los OE busquen proveedores que les proporcionen servicios de TI independientes o servicios y tecnologías de ciberseguridad complementarios. Los servicios básicos de TI pueden incluir la gestión de dispositivos y redes, el almacenamiento seguro o la copia de seguridad de datos en servidores remotos (en la nube) o locales. Los servicios de seguridad cibernética pueden incluir: servicios de investigación/forenses, servicios de auditoría, servicios de ingeniería de seguridad cibernética, operaciones de seguridad cibernética y/u otros servicios y tecnologías para comprobar vulnerabilidades.⁶ Del mismo modo, los OE pueden contratar a proveedores para que supervisen los sistemas en busca de indicios de ataques u otros problemas.

Otros usos de la tecnología en las elecciones

Algunos organismos de gestión electoral adquieren hardware, software y servicios relacionados para otros procesos y necesidades. Estos pueden incluir:

- Herramientas de educación del votante, incluidas aplicaciones para teléfonos inteligentes.
- Software especial de gestión electoral, incluidas herramientas para el registro de candidatos, informes y seguimiento de la financiación de campañas y otros procesos.
- Software de gestión de casos utilizado para la resolución de disputas electorales.
- Amplia gama de servicios de tecnología de la información, incluida la capacitación, el mantenimiento y el servicio de las tecnologías internas del organismo de gestión electoral.
- Tecnologías relacionadas con las auditorías postelectorales, que pueden incluir escáneres ópticos, software analítico u otras herramientas.

2. Mercado tecnológico electoral: Panorama de los proveedores

A medida que el uso de la tecnología en las elecciones amplía su alcance y se extiende a nuevos países, el panorama de los proveedores ha evolucionado en los últimos años. Varios vendedores a gran escala se especializan en el **suministro** de tecnologías, obteniendo equipos de diferentes desarrolladores o fabricantes, distribuyendo equipos por todo el país y prestando servicio a esas tecnologías en la práctica (a menudo a través de filiales locales). En su mayor parte, estas empresas de suministro/logística no se abordan en este documento, aunque los principios que se exponen a continuación siguen siendo aplicables a la contratación y a las soluciones tecnológicas que proporcionan.

⁵ Para más información sobre datos abiertos y principios afines, consulte <https://openelectiondata.net/es/guide/principles/>

⁶ Tenga en cuenta que los servicios de pruebas a veces son ofrecidos por los fabricantes o desarrolladores de ese hardware o software electoral concreto. En este caso, los proveedores están probando las vulnerabilidades de los productos que fabrican y mantienen, lo que da lugar a posibles conflictos de intereses y problemas de responsabilidad, transparencia e integridad del sistema. Por ejemplo, consulte: [El problema del hash en las elecciones: "Cuando el propio sistema de verificación de la integridad del software electoral carece de integridad." \(en inglés\)](#).

En cambio, este documento se centra en los fabricantes, desarrolladores y proveedores de servicios de software de tecnologías electorales que venden directamente a los organismos de gestión electoral y a otros implementadores/donantes electorales. Muchas empresas se centran en un tipo de servicio o producto (por ejemplo, sistemas de votación por Internet o sistemas biométricos de registro de votantes), mientras que cada vez son más las que ofrecen sistemas para múltiples procesos. Algunas empresas promueven las llamadas soluciones "de extremo a extremo" que soportan el registro electrónico (a menudo biométrico) de votantes, la verificación de votantes y el voto electrónico.

En la actualidad, la gran mayoría de los proveedores de tecnología electoral son empresas privadas, muchas de las cuales suministran a múltiples países y elecciones. Muchas de estas empresas están constituidas en los Estados Unidos (EE.UU.) o en Europa y, por lo tanto, entran dentro de esas jurisdicciones legales. Además, varias empresas más pequeñas con sede fuera de EE.UU. y Europa han suministrado tecnologías electorales a los organismos de gestión electoral, incluidas varias de América Latina, Asia y Eurasia. Las adquisiciones y fusiones de empresas de tecnología electoral se han hecho cada vez más comunes en los últimos años (especialmente en el mercado estadounidense), ampliando los tipos de tecnología ofrecidos por determinados proveedores, pero también reduciendo la competencia en el mercado e introduciendo nuevos problemas de seguridad (por ejemplo: el pirateo de una empresa importante afecta a más elecciones).⁷

Algunos organismos gubernamentales, OE o empresas públicas de países como Bielorrusia, Brasil, India, Kirguistán, Rusia, Suiza y otros, han desarrollado tecnologías electorales para sus propias elecciones.⁸ Algunos, como India y Rusia, han exportado esa tecnología a otros países, ya sea a precio de costo o gratuitamente, como parte de la diplomacia internacional. Aunque estas opciones relativamente más baratas son bienvenidas para muchos OE, estos proveedores gubernamentales no parecen haber desarrollado un mercado fuerte para sus productos y servicios más allá de sus propios países: dicha tecnología exportada se limita a menudo a unos pocos casos piloto o a un uso nacional en sólo un puñado de otros países.

En muchos países, las empresas nacionales prestan a veces servicios tecnológicos más sencillos y a menor escala, como soporte de sitios web, ciberseguridad, bases de datos sencillas y, en algunos casos, software de notificación de resultados. Del mismo modo, los implementadores electorales internacionales crean ocasionalmente opciones tecnológicas electorales a pequeña escala utilizadas por los OE.

⁷ En el mercado estadounidense, la amenaza de litigios ha puesto en jaque a algunos competidores que se introducían en el mercado y ha disuadido a los OE de abandonar la tecnología más antigua, como se detalla aquí: <https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it>. Al mismo tiempo, la fusión de empresas de tecnología electoral ha suscitado preocupación por los riesgos de piratería informática. Más información: <https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html?searchResultPosition=1>.

⁸Un pequeño número de OE subnacionales (estatales) de Estados Unidos han creado su propia tecnología, principalmente para uso de los votantes en el extranjero y militares. <https://verifiedvoting.org/election-system/in-house-remote-ballot-marking-systems-and-internet-voting-systems/>.

Nuevas empresas de tecnología electoral: La rampa de acceso a las nuevas tecnologías

Una parte mucho menor del mercado corresponde a las empresas emergentes de tecnología electoral, que desarrollan y comercializan nuevos productos. A menudo, las empresas emergentes persiguen una nueva solución tecnológica (como el voto por Internet o móvil) en lugar de intentar competir con tecnologías electorales más establecidas y basadas en hardware (como las máquinas de votación electrónica o los escáneres).

Las empresas emergentes que comercializan nuevas tecnologías suelen seguir un camino similar para introducirse en el mercado electoral. Muchas presionarán a legisladores, funcionarios electorales u otros responsables para promover la necesidad de una nueva tecnología y presentar su solución. Algunas empresas emergentes buscarán el uso en elecciones informales, no vinculantes o no gubernamentales (como sindicatos, elecciones estudiantiles, etc.) para probar y establecer casos de uso de sus tecnologías. Después, muchos proveedores buscan su uso en elecciones más importantes, como las primarias de los partidos, las elecciones a los órganos de gobierno regionales o su uso en procesos gubernamentales oficiales, como la votación legislativa a distancia o la votación en la Suprema Corte utilizada durante la pandemia COVID-19.

Una vez establecido un historial, las empresas emergentes pueden promover su uso en elecciones formales y constitucionales organizadas por los organismos de gestión electoral. En estos primeros casos, las nuevas tecnologías suelen proporcionarse gratuitamente o a muy bajo costo a los organismos de gestión electoral que desean probar nuevas soluciones. Las empresas de nueva creación, incluidas las que venden nuevas tecnologías o prestan servicios gratuitos, deben atenerse a las mismas normas y principios que los proveedores más establecidos, incluidas pruebas rigurosas, estudios de viabilidad y transparencia.

Es cada vez más frecuente que las plataformas de redes sociales desempeñen un papel más importante como proveedores de tecnología electoral mediante la creación y el despliegue de herramientas de información y búsqueda de votantes. Aunque los OE no suelen compensar a estas plataformas por este servicio, si amplían su función para facilitar otros procesos electorales (como el registro de votantes), su función y su tecnología deberían regirse por las mismas normas y principios que la tecnología electoral pagada o donada.

3. Principios de integridad en la tecnología electoral

Como se describe en la Sección I, las tecnologías suelen estar profundamente entrelazadas en los procesos electorales, incluso en los más fundamentales para la integridad electoral. La introducción de tecnología (ya sea hardware, software o servicios) en el proceso electoral no elimina la necesidad de normas universales de integridad que fomenten la

confianza pública en las elecciones y sus resultados. Tal y como se analiza a fondo en ***Principios y directrices generales relacionados con las TIC y las elecciones***, las tecnologías electorales deben cumplir los mismos principios que rigen las elecciones democráticas, tal y como se prescribe en las leyes y compromisos internacionales, regionales y nacionales. Esto incluye: el mantenimiento de la integridad (incluida la seguridad), el voto secreto y la igualdad del voto, la universalidad, la transparencia, la responsabilidad y la confianza pública en las elecciones.⁹ Como se expone en dicho documento, estos principios deben mantenerse en cada paso de la adopción de la tecnología: 1) a medida que se evalúa y define la necesidad tecnológica única y específica de cada país; 2) a medida que se determinan y adquieren las especificaciones de una solución tecnológica; 3) a medida que se selecciona un proveedor adecuado y competitivo; y 4) a medida que el proveedor desarrolla, aplica y mantiene la herramienta. Como se indica en el documento, ***estos principios se aplican no sólo a los procesos de toma de decisiones y adquisición del organismo de gestión electoral u otros organismos públicos, sino también a los vendedores, fabricantes, desarrolladores y proveedores de servicios de tecnologías electorales y a los productos y servicios que proporcionan.***

Las normas analizadas en ***Principios y directrices generales sobre las TIC y las elecciones*** son muy aplicables y se extienden a las mejores prácticas claras relacionadas con la tecnología electoral básica y sus proveedores. Estas consideraciones pueden servir como base de referencia de las normas del sector, proporcionando tanto un conjunto de metas que los proveedores deben alcanzar como un conjunto de medidas que los OE y otros deben tener en cuenta a la hora de comparar proveedores en un proceso de licitación. En la práctica, estas consideraciones pueden incluir:

1. **Viabilidad.** Una consideración destacada a la hora de evaluar la viabilidad de las soluciones tecnológicas es si una tecnología se adapta o no a un contexto y puede resolver eficazmente los problemas identificados. A menudo, las tecnologías desarrolladas para un contexto general y/o desplegadas en otros países pueden no ser flexibles y/o eficientes para resolver las necesidades específicas de otro país o para satisfacer otras consideraciones específicas que se enumeran a continuación. En este sentido, es fundamental probar las tecnologías para garantizar su funcionalidad y seguridad básicas, así como ponerlas a prueba en condiciones reales para asegurarse de que funcionarán en el contexto específico de un país. Los proveedores deben comprometerse a adaptar y probar su tecnología para garantizar su aplicabilidad y adecuación al contexto específico del país.
2. **Soberanía y autonomía de los OE.** Como principales ejecutores de las elecciones, los OE son los responsables finales de los procesos electorales y de su aplicación. Esto requiere que los OE tengan una capacidad significativa para decidir sobre las soluciones, seleccionar y supervisar a los proveedores y, en última instancia, solucionar los problemas y gestionar las soluciones tecnológicas para la sostenibilidad a largo plazo. Por un lado, los organismos

⁹ Consulte el documento Principios y directrices, p. 2.

de gestión electoral deben tener capacidad tecnológica interna (incluido personal experto) que pueda evaluar y asesorar sobre las especificaciones tecnológicas y la selección de herramientas, así como solucionar los problemas que surjan. Por otro lado, los proveedores de tecnología deben proporcionar formación suficiente al personal tecnológico del organismo de gestión electoral y garantizar el nivel necesario de colaboración, transparencia y acceso para que éste pueda supervisar y gestionar eficazmente la aplicación.

3. **Sostenibilidad.** Idealmente, los proveedores deben comprometerse a proporcionar soluciones tecnológicas sostenibles que sigan siendo viables, adaptables y responsables a lo largo de varios ciclos electorales. El costo total de propiedad (CTP) y los costos del ciclo de vida de una tecnología deben ser claros para el OE y transparentes para las demás partes interesadas en el proceso electoral. La clave de la sostenibilidad es evitar el "bloqueo del proveedor", que impide a los organismos de gestión electoral cambiar de proveedor (o de solución tecnológica) sin perder el control o el acceso a partes clave del proceso electoral o a los datos. Las estructuras de costos que requieren servicios de "arrendamiento" o "suscripción" (que pueden estar sujetos a aumentos de costes) para seguir teniendo acceso pueden hacer que la tecnología sea menos sostenible y amenazar la soberanía del OE sobre los procesos electorales. Esto incluye precios abusivos por nuevo hardware, actualizaciones de software o servicios adicionales para solucionar problemas, sustituir o ampliar equipos, o mantener la seguridad actualizada. La capacitación y la colaboración sustantivas que mejoran la autonomía tecnológica del OE con el paso del tiempo también son clave para la sostenibilidad.
4. **Propiedad de los datos, rendición de cuentas y responsabilidad.** Como se mencionó anteriormente, los OE y los proveedores deben garantizar que los datos electorales sensibles (incluidas las listas de votantes, la información de identificación personal y los datos biométricos, los votos emitidos, los resultados tabulados y los cálculos de asignación de puestos) permanezcan bajo el control del OE. Los datos deben recopilarse y almacenarse de modo que permanezcan sujetos a la jurisdicción legal del país y sujetos a revisión judicial en caso de procedimientos de disputa electoral.¹⁰ Además, el país de incorporación de una empresa tecnológica puede ser relevante para comprender las responsabilidades adicionales y las medidas legales de rendición de cuentas. Por ejemplo, las empresas pueden estar sujetas a leyes y reglamentos locales que pueden tener repercusiones positivas o negativas. Por un lado, las normativas empresariales o de privacidad del país en el que están constituidas pueden establecer normas más estrictas de transparencia. Por otro lado, algunos gobiernos del país de origen pueden aplicar leyes

¹⁰ Consulte el documento Principios y directrices, p. 11

locales para acceder a datos sensibles -incluidos los datos de identificación personal de los votantes- que obren en poder de la empresa.

5. **Transparencia y confianza pública.** Como en cualquier otro aspecto del proceso electoral, la transparencia es clave en el uso de las tecnologías electorales. Los procesos de adquisición, el diseño de los productos, el código fuente (ya sea totalmente abierto o facilitado a revisores independientes seleccionados) y los acuerdos contractuales deben prever la transparencia pública, la supervisión y el seguimiento de los productos tecnológicos.¹¹ Más allá de la propia tecnología, la transparencia sobre los proveedores también es importante para fomentar la confianza pública y combatir la desinformación. En las últimas elecciones, actores de mala fe han difundido

¹¹ En ocasiones, los códigos fuente son totalmente públicos, para generar una mayor confianza. Otras veces, el código fuente se facilita a un grupo selecto de supervisores o auditores independientes. Para más información sobre el código fuente y otras medidas de transparencia técnica, consulte en NDI "[Monitoreo de Tecnologías Electrónicas en Procesos Electorales](#)" (2007) (en inglés); En IFES y NDI, "[Implementación y Supervisión de Tecnologías de Votación y Recuento Electrónicos](#)" (2013) (en inglés).

Mitigar los riesgos tecnológicos en las elecciones

En muchos casos, la tecnología puede contribuir a que la administración electoral sea más eficaz y transparente. Sin embargo, la introducción de la tecnología conlleva nuevos riesgos para la seguridad y la integridad electorales, así como para los derechos de las personas. Si las tecnologías fallan, los procesos de votación básicos pueden verse afectados y la confianza en las elecciones puede verse irremediablemente afectada. Esto es especialmente cierto en el caso de los procesos más importantes para las elecciones y la confianza en las mismas: registro y verificación de los votantes, votación, recuento, tabulación, gestión de resultados y auditorías, o tecnología de recogida de datos personales identificables de los votantes. Dependiendo del tipo de tecnología, los procesos que automatizan y los datos que implican, puede ser necesario un mayor nivel de cuidado y mitigación de riesgos.

Los riesgos potenciales vienen de todas partes: sabotaje intencionado; planificación o pruebas deficientes; déficits de presupuesto, capacitación o infraestructura tecnológica; etc. Los fallos pueden provenir de la propia tecnología, del proveedor, de una vulnerabilidad de la cadena de suministro o de un OE u otro ejecutor. Así pues, todos los agentes clave -incluidos los vendedores- tienen un papel que desempeñar en la mitigación del riesgo.

El papel de los OE en la mitigación de riesgos - Los OE desempeñan un papel primordial en la mitigación de los riesgos que traen consigo las nuevas tecnologías. Además de abordar las deficiencias en infraestructura y capacidad tecnológica, las carencias presupuestarias o la falta de inversión en ciberseguridad, el OE también debe garantizar que: solo se adopten las herramientas adecuadas; que todo el proceso de adopción (incluidas la licitación, la selección, las pruebas y la certificación) sea transparente; que existan redundancias para evitar una ruptura de los procesos electorales clave; y que se garantice una supervisión independiente mediante auditorías independientes y un seguimiento no partidista.

El papel de los proveedores en la mitigación de riesgos - Como apoyo y complemento de las políticas de los organismos de gestión electoral, los proveedores son socios clave a la hora de garantizar una mitigación de riesgos adecuada para las tecnologías electorales. Esto incluye practicar una total transparencia en torno a sus propias vulnerabilidades y estrategias internas de mitigación; comprometer los recursos apropiados, la apertura y la responsabilidad en el diseño, las pruebas y la auditoría de la tecnología; y trabajar con los OE para proporcionar capacitación suficiente y facilitar las redundancias planificadas.

desinformación dirigida a las empresas de tecnología electoral y a sus propietarios para sembrar la desconfianza en los procesos electorales.¹² Para demostrar imparcialidad, combatir la desinformación y fomentar la confianza pública en las tecnologías electorales, deben hacerse públicos los

detalles sobre las empresas, como la propiedad y otras obligaciones financieras, y las políticas internas de debida diligencia.¹³ Además, deben revelarse los posibles conflictos de intereses, los incidentes de seguridad y otras cuestiones clave.

6. **Competencia, experiencia y capacidad.** Reconociendo la importancia y la sensibilidad de las tecnologías electorales, los proveedores deben estar profundamente comprometidos con la realización de la debida diligencia necesaria y con la entrega de una solución tecnológica plenamente satisfactoria. Más allá del simple costo, los proveedores deben demostrar su viabilidad como empresa, la fiabilidad de su tecnología y su nivel de experiencia cuando su tecnología se tenga en cuenta en un proceso de licitación. Cualquier controversia o historial de litigios relacionados con el proveedor también deben ser revelados y considerados para evitar posibles problemas de entrega o amenazas a la confianza pública en las tecnologías electorales.
7. **Respeto de los derechos humanos, la seguridad y la privacidad.** Las preocupaciones más amplias por los derechos humanos, la seguridad y la privacidad también deben abordarse e incorporarse a las políticas de la empresa, el diseño de productos y la debida diligencia.¹⁴ La adopción y el diseño de herramientas deben ser inclusivos y tener en cuenta los riesgos y preocupaciones específicos de las comunidades marginadas, así como los derechos más amplios, la privacidad y los principios electorales, incluidos el secreto, la igualdad y la universalidad del voto. Para garantizar la integridad del proceso de votación, deben existir suficientes defensas de seguridad y redundancias (tanto en el diseño de la tecnología como por parte del proveedor y del organismo de gestión electoral) para garantizar que los problemas no desbaraten los procesos electorales básicos ni erosionen la confianza pública.

Cuando se utilizan tecnologías para recoger y almacenar datos de los votantes -incluidos los datos personales y biométricos- deben tenerse en cuenta medidas y principios adicionales. Esto incluye políticas y prácticas que garanticen que la recogida, la transmisión, el almacenamiento y la protección de los datos son seguros y no corren riesgo de piratería, uso indebido o vigilancia.

¹² La desinformación fue especialmente grave en Estados Unidos, donde las inversiones opacas de capital privado y la propiedad de empresas del mercado estadounidense alimentaron las teorías conspirativas y sembraron una gran desconfianza en los procesos electorales.

¹³ Algunos promotores de la transparencia animan a revelar las participaciones superiores al 5% para que los OE, los responsables de la toma de decisiones y el público sean conscientes de cualquier conflicto de intereses real o percibido. En Estados Unidos, donde la desinformación sobre la propiedad generó desconfianza en las elecciones, algunos legisladores federales y estatales empezaron a exigir información sobre la propiedad de los proveedores electorales a través de investigaciones legislativas y requisitos de licitación. Consulte <https://www.warren.senate.gov/oversight/letters/warren-klobuchar-wyden-and-pocan-investigate-vulnerabilities-and-shortcomings-of-election-technology-industry-with-ties-to-private-equity>

¹⁴ Consulte el documento Principios y directrices, p. 16

Riesgos de corrupción en la adopción y adquisición de tecnologías electorales electrónicas

Como ocurre con cualquier inversión de alto costo, sigue existiendo un mayor riesgo de corrupción e influencia indebida en la contratación de recursos para las elecciones. De hecho, ha habido varios casos notorios y condenas por soborno de proveedores electorales y corrupción de funcionarios. La tecnología electoral se enfrenta a este riesgo a lo largo de su adopción, pero puede mitigarse mediante una mayor transparencia, una toma de decisiones inclusiva y la oportunidad de que el público realice aportaciones, así como una responsabilidad y supervisión continuas de la tecnología electoral. Estos principios son clave *incluso cuando* la tecnología puede ser donada o proporcionada gratuitamente por un proveedor.

Revisión de la tecnología electoral

El rendimiento y el uso de la tecnología deben ser auditados y revisados a fondo para determinar el grado en que las herramientas satisfacen las necesidades de las y los ciudadanos y la integridad de las elecciones y determinar si deben continuar.

Decisión de Adoptar Tecnología Electoral

Debe basarse en las necesidades de las y los ciudadanos y la integridad de las elecciones, no en presión o donativos por parte de proveedores o en beneficio personal.



Mitigación de la corrupción en la adopción de EET

Proceso de Adquisiciones y Selección

Debe ser un proceso totalmente transparente, que exija que los proveedores divulguen quiénes son en realidad sus dueños o "beneficiarios efectivos" y que ofrezca una justificación clara para la selección.

Desarrollo de ofertas

Las convocatorias deben ser abiertas y competitivas. Las especificaciones deben ser determinadas por expertos en tecnología del organismo electoral, y contar con la oportunidad de recibir comentarios del público.

La recogida de datos biométricos -que es mucho más delicada debido a la información altamente específica y personalmente identificable que se conserva- exige normas aún más estrictas de evaluación y mitigación de riesgos, el consentimiento informado de cómo se utilizarán esos datos y una mayor garantía de seguridad en el tratamiento de los datos y la privacidad. Por ejemplo: puede proponerse el uso de software de reconocimiento facial para registrar y verificar a los votantes. Sin embargo, los gobiernos han abusado de este tipo de software y, en nombre de la seguridad pública, lo utilizan para vigilar las actividades cotidianas de los ciudadanos. El uso de una tecnología tan sensible en el proceso electoral exige una mayor supervisión, la aportación de organizaciones de defensa de los derechos de los ciudadanos, así como de expertos en privacidad y tecnología, para garantizar que no se abusa de dicha tecnología.

4. Principios en la práctica: Regulación de proveedores, requisitos y políticas internas

Reconociendo el impacto que la tecnología puede tener en el éxito o el fracaso de los procesos electorales, aumentan los esfuerzos por aplicar principios más amplios de buena gobernanza, ciberseguridad y derechos humanos al diseño, la fabricación y la adquisición de tecnología electoral.¹⁵ A medida que el campo de la tecnología electoral crece y evoluciona, han surgido diversos esfuerzos para regular, coordinar y promover las mejores prácticas entre los proveedores. Estos enfoques pueden servir de ejemplo y de posibles vías para ampliar las normas y prácticas de integridad electoral entre los proveedores de tecnología electoral. Entre ellos figuran:

Normativa gubernamental

Algunos gobiernos prueban y certifican la tecnología electoral de diversos proveedores. Uno de los principales ejemplos es Estados Unidos, donde la Comisión de Asistencia Electoral, a través de laboratorios acreditados a nivel federal, prueba y certifica las máquinas de votación electrónica. Aunque la ley federal no lo exige, el proceso supone un fuerte incentivo para que los proveedores cumplan las normas federales y obtengan la "certificación" oficial cuando se presentan a las licitaciones para suministrar tecnología a las jurisdicciones electorales subnacionales de Estados Unidos.

Otros gobiernos establecen normativas que imponen determinadas garantías en materia de derechos humanos y privacidad, requisitos de transparencia u otras prácticas que pueden aplicarse a las empresas constituidas en ese país o que hacen negocios en él. Por ejemplo, el [Reglamento General de Protección de Datos \(RGPD\) de 2018 de la Unión Europea](#) impone estrictas protecciones de la privacidad de los datos a las organizaciones o empresas con presencia en la UE o que manejan datos sobre ciudadanos de la UE (independientemente de que esas entidades tengan o no su sede en la UE). Esta normativa puede aplicarse a las tecnologías electorales utilizadas en la UE relacionadas con el registro o la verificación de los votantes (incluida la identificación biométrica). Algunos proveedores de tecnología han respondido con nuevos protocolos y cambios tecnológicos para cumplir estas normas emergentes, incluido el cumplimiento de las medidas de recopilación, almacenamiento y privacidad de datos.¹⁶

Mandatos y normas de contratación

Algunos gobiernos, organismos electorales, proveedores de asistencia u otros actores pueden establecer normas de contratación que obliguen a los proveedores licitadores a respetar determinados principios. Los organismos gubernamentales pueden establecer recomendaciones para las tecnologías electorales, como las [Recomendaciones sobre normas para el voto electrónico del Consejo de Europa](#). En algunos casos, los donantes de

¹⁵ Consulte el documento Principios y directrices, p. 3

¹⁶ Consulte <https://www.biometricupdate.com/202010/genkey-updates-biometric-database-software-to-meet-eu-gdprs-right-to-be-forgotten-requirement>

proyectos electorales han desarrollado sus propias normas para la adquisición de tecnología electoral.

En muchos casos, los requisitos de contratación están relacionados con principios más amplios de buena gobernanza y/o ciberseguridad. En su práctica de contratación global, que incluye una gran parte de la tecnología electoral, el Programa de las Naciones Unidas para el Desarrollo (PNUD) establece requisitos de [calificación y elegibilidad](#) para cualquier proveedor que desee optar a contratos. Al mismo tiempo, todos los proveedores licitadores deben comprometerse con el [Código de Conducta](#) para Proveedores de las Naciones Unidas, que exige prácticas laborales, de derechos humanos, medioambientales y anticorrupción/éticas sólidas.

Coordinación de proveedores

Recientemente, a medida que ha ido creciendo la preocupación por la ciberseguridad en torno a la tecnología electoral, los organismos gubernamentales (a nivel regional, nacional y subnacional) han intentado coordinar a los distintos vendedores para compartir información, promover las mejores prácticas y establecer normas más estrictas en el mercado. Por ejemplo, la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA, por sus siglas en inglés) de Estados Unidos convoca a los proveedores de tecnología electoral a través del [Consejo de Coordinación Sectorial](#) para compartir información y coordinar las amenazas a la ciberseguridad electoral.

Códigos de conducta y políticas corporativas voluntarias

Las empresas independientes y otras entidades pueden comprometerse voluntariamente con el [Pacto Mundial de las Naciones Unidas](#) estableciendo principios sobre derechos humanos, trabajo, medio ambiente y lucha contra la corrupción, lo que han hecho muchos proveedores de tecnología electoral. Algunos proveedores de tecnología electoral o de elecciones crean y publican sus propios códigos de conducta empresariales para prohibir las prácticas corruptas y poco éticas. Del mismo modo, algunos proveedores crean sus propias políticas corporativas, como la prohibición de donaciones políticas y la neutralidad política.

Estos ejemplos muestran los diversos enfoques -desde los requisitos legales y de licitación impuestos externamente, hasta el intercambio voluntario de mejores prácticas o la gobernanza interna- que han influido en la forma en que los proveedores aplican los principios de integridad electoral a su negocio y a su tecnología.

Conclusión

A medida que aumenta el uso de las tecnologías en las elecciones y evoluciona el mercado de proveedores de tecnología, se hace evidente la necesidad de adoptar principios rectores y mejores prácticas. Los principios comunes que rigen las elecciones democráticas se aplican no sólo a la tecnología electoral, sino también a las prácticas empresariales que subyacen a su desarrollo y aplicación. Más allá de estos principios, existen consideraciones e implicaciones prácticas que se deben tener en cuenta, tanto por parte de los OE como de los propios proveedores. Desde un punto de vista positivo, existen varios avances en la

promoción de normas, principios y buenas prácticas entre los proveedores de tecnología electoral, a través de la regulación y los requisitos de licitación, o mediante la educación voluntaria y la adopción de políticas internas. De cara al futuro, hay margen para una mayor colaboración con los proveedores -y con quienes contratan sus servicios- para promover los principios democráticos en la tecnología electoral.