

Principios y lineamientos generales relacionados con las TIC y las elecciones

*Un documento técnico de la DoP (Declaración de principios)
Aprobado en Bruselas, 15 de noviembre de 2021*

Tras una revisión y debate exhaustivos de los documentos preliminares de los Lineamientos, las organizaciones de la DoP reconocen a los Lineamientos como Documentos Técnicos para ayudar a la implementación de la Declaración de Principios. No requieren acciones por parte de los órganos políticos de las organizaciones que los respaldan (como asambleas, consejos o juntas directivas), aunque dichas acciones son bienvenidas.

Índice

Introducción	1
Principios para unas elecciones auténticas y TIC electorales.....	5
Cumplimiento de las obligaciones y compromisos internacionales para unas elecciones democráticas inclusivas.....	5
Transparencia	7
Rendición de cuentas	10
Seguridad digital.....	11
Responsabilidades de las partes interesadas [y rendición de cuentas]	13
El Organismo Electoral (OE).....	14
Otras partes interesadas nacionales	16
Fabricantes y vendedores de E-TIC.....	17
Donantes internacionales y proveedores de asistencia técnica	18
Resumen.....	20

Introducción

En los últimos años se ha prestado una atención considerable a las oportunidades y los riesgos que implica la introducción y el uso de las nuevas tecnologías de la información y la comunicación en el ámbito electoral (e-TIC). El progreso tecnológico ha dado lugar a una creciente variedad de soluciones e-TIC disponibles para automatizar aspectos específicos del proceso electoral. Su adopción y utilización ha destacado tanto las auténticas contribuciones positivas que pueden ofrecer las e-TIC, como la necesidad de que éstas se asienten sólidamente en un marco jurídico y operativo adecuado que garantice su uso eficaz y basado en principios.¹

En este documento, las e-TIC se refieren a cualquier proceso digital que sustituya a los procesos electorales manuales, incluidas las tecnologías para el registro de votantes y candidaturas, la gestión del voto y de los resultados. Los procesos de e-TIC aquí tratados no incluyen el uso de Internet o de plataformas de redes sociales con fines políticos, los cuales constituyen un tema aparte.²

La comunidad de organizaciones que suscriben la Declaración de Principios para la Observación Electoral Internacional (DoP por sus siglas en inglés),³ tiene como misión apoyar y mejorar la integridad del proceso electoral, así como promover la confianza pública en el mismo. Como parte de esta misión, considera importante en este momento destacar cuáles son los principios fundamentales que deben sustentar los sistemas e-TIC. En este contexto, también es útil identificar y aclarar las responsabilidades de todas las partes interesadas en la adopción y aplicación de las e-TIC.

Los sistemas e-TIC están sujetos a los principios fundamentales que sustentan las elecciones democráticas, contenidos en la Carta Internacional de Derechos Humanos (que incluye la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos

¹ El informe del Secretario General de la ONU de 2019 sobre el Fortalecimiento de la función de las Naciones Unidas para mejorar la eficacia del principio de elecciones periódicas y auténticas y la promoción de la democratización hace hincapié en: 'Las Naciones Unidas no alientan ni desalientan a los Estados Miembros en cuanto a introducir innovaciones digitales en sus procesos operacionales. Sus posibilidades para aumentar la participación, reducir algunas irregularidades, y fortalecer la confianza pública pueden ser grandes. Al mismo tiempo, algunas de las conclusiones alarmantes esbozadas en informes anteriores han sido confirmadas por la experiencia reciente. Estas incluyen la importancia de garantizar, ante todo, la claridad en relación con el problema que debe resolverse mediante cualquier tecnología nueva, de dedicar tiempo suficiente a examinar la viabilidad técnica, financiera y política de la innovación mediante un amplio proceso consultivo, y de introducir gradualmente nuevas tecnologías que permitan realizar pruebas y ajustes exhaustivos. En esas pruebas también se deberían tener en cuenta las crecientes preocupaciones por la vulnerabilidad de las infraestructuras electorales nacionales a los ataques cibernéticos.'

https://dppa.un.org/sites/default/files/sg-electoral_assistance_report_final_20191114_e.pdf.

² El informe del Secretario General de la ONU de 2019 sobre la asistencia electoral de la ONU también hace una distinción deliberada entre la influencia que ejerce el internet, las redes sociales y las tecnologías digitales para las operaciones electorales. https://dppa.un.org/sites/default/files/sg-electoral_assistance_report_final_20191114_e.pdf.

³ 'Declaración de Principios para la Observación Internacional de Elecciones', suscrita el 27 de octubre de 2005 en las Naciones Unidas. Actualmente ha sido suscrita por 55 organizaciones de observación internacional. <https://www.ndi.org/sites/default/files/DoP-SPA.pdf>

Económicos, Sociales y Culturales, y el Pacto Internacional de Derechos Civiles y Políticos y sus dos Protocolos Facultativos), junto con otros compromisos internacionales y regionales. Éstos deben servir de guía no sólo para el diseño de los sistemas, sino también para su adopción, despliegue y uso. Estos sistemas son herramientas diseñadas para sustituir algunas de las funciones tradicionalmente manuales en el proceso electoral, por lo que deben cumplir los estándares que se aplican a las elecciones democráticas, en concreto, la integridad, el voto secreto, la universalidad e igualdad del voto, la transparencia, la responsabilidad y la confianza pública en las elecciones. Dada la naturaleza crítica de las infraestructuras TIC relacionadas con las elecciones y la enorme cantidad de datos generados, la seguridad de las e-TIC y la garantía del derecho a la privacidad son también cruciales para la integridad del proceso. Sólo si se garantiza que los sistemas e-TIC cumplen estos principios, las administraciones electorales y otras partes interesadas podrán aprovechar los beneficios potenciales de las e-TIC, reforzando así la confianza de los ciudadanos.

Los Estados, a través de su organismo electoral (OE), son responsables en última instancia de la credibilidad de las elecciones, incluida la adopción y aplicación de herramientas de e-TIC.⁴ Sin embargo, está surgiendo un consenso en torno a la idea de que los fabricantes y proveedores de e-TIC también tienen responsabilidades en lo que respecta al respeto de las libertades fundamentales y los derechos humanos asociados a los procesos electorales. Entre otros, los Principios Rectores sobre las Empresas y los Derechos Humanos de la ONU⁵ y el Panel de Alto Nivel sobre Cooperación Digital del Secretario General de la ONU⁶ han desarrollado una visión para seguir trabajando en este sentido.

Por último, los donantes y los proveedores de asistencia electoral deberían promover y trabajar para garantizar estos principios cuando consideren otorgar su asistencia a procesos electorales que impliquen la adopción de e-TIC.

Este documento ofrece una serie de principios y lineamientos generales que buscan ser de apoyo para el trabajo de las diversas comunidades que trabajan en el campo de las TIC y las elecciones. Esto incluye a los responsables de la elaboración de políticas que consideran la aplicación de las TIC en sus elecciones, los OE que buscan implementar soluciones de TIC, los proveedores de soluciones electorales de TIC, así como los observadores y otras partes interesadas en el proceso electoral.

⁴ Consejo de Europa - Recomendación de la Comisión de Ministros sobre estándares para el voto electrónico CM/Rec (2017)5. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f.

⁵ Las empresas tienen una diligencia debida en materia de derechos humanos. Esto significa que deben evitar vulnerar los derechos humanos de los demás y abordar las repercusiones negativas sobre los derechos humanos en las que estén implicados. Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Principios rectores sobre las empresas y los derechos humanos. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf. Consulte también la recomendación CM/Rec (2016)3 del Consejo de Europa a los Estados miembros sobre Derechos Humanos y Empresas. <https://edoc.coe.int/en/fundamental-freedoms/7302-human-rights-and-business-recommendation-cmrec20163-of-the-committee-of-ministers-to-member-states.html>.

⁶ Reporte del Panel de Alto Nivel sobre Cooperación Digital del Secretario General de la ONU, la era de la interdependencia digital, p.16. <https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-for-web.pdf>

La comunidad de la DoP, como red de organizaciones con amplia experiencia en el campo de las buenas prácticas electorales, ofrece estos lineamientos generales como contribución a todas las partes interesadas.⁷ Partiendo de estos lineamientos generales, la comunidad de la DoP pretende ofrecer otras recomendaciones dirigidas especialmente a las organizaciones de observadores, los OE, los legisladores/reguladores y la comunidad de donantes.

*"[L]a integridad electoral es, en su origen, un problema político. [...] [D]epende de la confianza de los ciudadanos en los procesos electorales y políticos. No basta con reformar las instituciones; hay que convencer a los ciudadanos de que los cambios son reales y merecen su confianza. La inclusión, la transparencia y la responsabilidad son fundamentales para desarrollar esa confianza."*⁸

Si se aplican correctamente, las e-TIC pueden facilitar una gestión eficaz y creíble de diferentes aspectos del proceso electoral, por ejemplo en el registro de votantes, la votación y la gestión de los resultados. Pueden ser herramientas para lograr una mayor inclusión de los votantes, una mayor transparencia del proceso y nuevos medios para supervisar el trabajo de la administración electoral. Sin embargo, también pueden subvertir la integridad electoral como consecuencia de un fallo de la tecnología, una manipulación malintencionada o un proceso de adopción precipitado, o crear retos y aumentar la complejidad, lo que a veces lleva a debilitar un factor clave del proceso electoral: la confianza.

Unas elecciones legítimas son aquellas en las que el resultado refleja las opciones libremente expresadas por el pueblo.⁹ La confianza política -la creencia en la integridad de las instituciones políticas y del régimen del que forman parte- es un indicador fundamental de la legitimidad política. La confianza generalizada en la legitimidad de la administración electoral es una condición necesaria para la confianza en la integridad de unas elecciones. La confianza pública es un elemento esencial para el uso de las e-TIC. Un enfoque gradual de su introducción, junto con pruebas exhaustivas, verificabilidad y total transparencia, puede ayudar a desarrollar la confianza pública en las soluciones e-TIC.¹⁰

Cuando existe un nivel significativo de desconfianza o descontento con la administración electoral, la introducción de las e-TIC puede resultar problemática y disminuir aún más la confianza del público en las elecciones. Sin embargo, la adopción de las e-TIC no puede resolver los problemas políticos que pueden estar en el origen de la falta de confianza en la integridad de unas elecciones. Por lo tanto, es necesario valorar cuidadosamente y de forma independiente las expectativas de lo que podrían ser los beneficios potenciales de la

⁷ En la referencia 17 figura una lista de los documentos relativos a las e-TIC electrónicas elaborados por las organizaciones signatarias de la DoP.

⁸ Comisión Global sobre Elecciones, Democracia y Seguridad, Profundizando la Democracia: Una estrategia para mejorar la integridad de las elecciones en todo el mundo (2012), párr. 28/29.

⁹ Informe del Secretario General de la ONU sobre la asistencia electoral de la ONU (2017) A/72/260, párr. 28. <https://digitallibrary.un.org/record/1302192?ln=en>
Halff, Maarten. 2015. Confianza en las elecciones y aceptación de los resultados. Informe político de la Iniciativa de Integridad Electoral. Ginebra: Fundación Kofi Annan.
<https://www.kofiannanfoundation.org/app/uploads/2016/06/Confidence-in-elections-and-the-acceptance-of-results.pdf>

¹⁰ OSCE/ODIHR Handbook for the observation of new voting technologies, <https://www.osce.org/odihr/elections/104939>.

adopción de un nuevo sistema de e-TIC. Será responsabilidad compartida de todas las partes interesadas, incluidos los partidos políticos, no disminuir la confianza en los sistemas e-TIC si se han seguido todas las buenas prácticas.

El Panel de Alto Nivel sobre Cooperación Digital, convocado por el Secretario General de la ONU en 2018, afirma: "Hay una necesidad urgente de examinar cómo los marcos y convenciones de derechos humanos consagrados por el tiempo -y las obligaciones que se derivan de esos compromisos- pueden guiar las acciones y políticas relacionadas con la cooperación digital y la tecnología digital." El grupo exhorta al Secretario General de la ONU a iniciar un proceso en el que se recaben las opiniones de todas las partes interesadas sobre cómo pueden aplicarse de forma significativa los derechos humanos para garantizar que las tecnologías digitales nuevas y emergentes no provoquen brechas en la protección. El informe señala que, si bien los Estados tienen la obligación de proteger los derechos y proporcionar recursos, el sector privado también tiene cada vez más la responsabilidad de evaluar los riesgos y el impacto de sus acciones sobre los derechos humanos. Más recientemente, en diciembre de 2020, la Comisión de Venecia del Consejo de Europa ha adoptado una serie de principios¹¹ que deben ser respetados por los legisladores, reguladores y otros actores implicados en el uso de las tecnologías digitales en las elecciones, que hacen hincapié en la necesidad de un enfoque respetuoso con los derechos humanos; los derechos humanos y las libertades fundamentales deben trasladarse al entorno digital.

Como ya se ha mencionado anteriormente, se les aplican los principios fundamentales que sustentan las elecciones democráticas, en concreto la integridad, el voto secreto, la universalidad/inclusividad e igualdad del voto, la transparencia, la rendición de cuentas y la confianza pública en el proceso. Algunos principios fundamentales pueden integrarse en el diseño de un sistema, lo que hace aún más probable que se respeten cuando el sistema esté en funcionamiento. Es importante, por tanto, que los proveedores del sector comercial también tengan en cuenta estos principios a la hora de plantearse la producción de nuevos sistemas de e-TIC.

La Comisión Global sobre Elecciones, Democracia y Seguridad hizo hincapié en la importancia de la transparencia, la rendición de cuentas y la confianza pública como los aspectos más relevantes para la integridad de unas elecciones y la base de la confianza pública.

La transparencia de los sistemas e-TIC ha sido una preocupación prominente y un reto para las partes interesadas en las elecciones. A menudo, los sistemas han resultado ser "cajas negras", fuera del escrutinio público, lo que dificulta saber si la voluntad de los votantes se refleja fielmente en los resultados electorales. La falta de inclusión en el proceso electoral, incluidos los debates y decisiones clave en torno a la adopción de las e-TIC, tiene un impacto negativo en la transparencia general del proceso. Del mismo modo, la falta de una rendición de cuentas clara en el uso de los sistemas e-TIC plantea un serio desafío a la transparencia y la credibilidad. En caso de que se impugnen los resultados, los tribunales nacionales necesitarán conocer en detalle las complejidades y el funcionamiento de las e-TIC. La verificabilidad y las pruebas deben estar bien definidas para ayudar a los tribunales a resolver las disputas electorales de forma rápida y que genere confianza.

¹¹ Comisión de Venecia, Principios para el uso de las tecnologías digitales en los procesos electorales en respeto de los derechos fundamentales.
[https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2020\)037-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2020)037-e)

Principios para unas elecciones auténticas y TIC electorales

La Declaración de Principios (DoP) establece que la observación internacional de elecciones es una expresión del interés de la comunidad internacional en apoyar las elecciones democráticas como parte del desarrollo democrático, incluido el respeto de los derechos humanos y el Estado de Derecho. Puede mejorar la integridad de los procesos electorales al disuadir y sacar a la luz irregularidades y fraudes y ofrecer recomendaciones para mejorar los procesos electorales. Puede fomentar la confianza pública, según proceda, promover la participación electoral y mitigar la posibilidad de conflictos relacionados con las elecciones. También sirve para mejorar el entendimiento internacional mediante el intercambio de experiencias e información sobre el desarrollo democrático.

La comunidad de la DoP representa una constelación de organizaciones internacionales, intergubernamentales, regionales y sin fines de lucro, cada una con un mandato y un alcance geográfico diferentes. Celebrada en las Naciones Unidas en 2005, la Declaración de Principios para la Observación Electoral Internacional, junto con el Código de Conducta para los Observadores Electorales Internacionales, sientan las bases de una observación electoral internacional creíble y cuentan ya con el respaldo de 55 organizaciones intergubernamentales e internacionales¹² comprometidas con la mejora de la observación electoral internacional. Al respaldar la declaración, los signatarios comparten los valores fundamentales de las elecciones democráticas y de la observación electoral internacional independiente. Una de las funciones que desempeña la DoP es estudiar las tendencias emergentes, como la introducción de las e-TIC en las elecciones.

Cumplimiento de las obligaciones y compromisos internacionales para unas elecciones democráticas inclusivas

Unas elecciones democráticas auténticas abarcan una gran variedad de derechos humanos y libertades fundamentales que deben ejercerse de forma permanente sin discriminación por motivos de raza, color, sexo, lengua, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento u otra condición, discapacidad, orientación sexual e identidad de género, y sin restricciones arbitrarias e irrazonables.

Los principios democráticos de unas elecciones democráticas auténticas se enuncian en la Carta Internacional de Derechos Humanos, complementada por otros tratados e instrumentos internacionales y regionales. Este cuerpo jurídico incluye otros derechos humanos -por ejemplo, el derecho a la privacidad- que, si bien no son de naturaleza explícitamente electoral, son pertinentes cuando se consideran las elecciones como procesos cíclicos amplios, participativos e inclusivos y no como acontecimientos aislados.¹³

El voto secreto, la integridad y la seguridad, la universalidad y la igualdad del voto, la transparencia, la rendición de cuentas y la confianza pública en el proceso son los principios básicos para la evaluación de unas elecciones. La Comisión Global sobre Elecciones, Democracia y Seguridad describe unas elecciones con integridad como "cualquier elección

¹² https://www.ndi.org/declaration_endorsing_orgs

¹³ Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos y el Centro Carter, El Plan de Acción de Derechos Humanos y Normas Electorales (2017). https://www.ohchr.org/Documents/Issues/Democracy/Elections/POA_EN.pdf

que se base en los principios democráticos del sufragio universal y la igualdad política, tal y como se reflejan en las normas y acuerdos internacionales, y que sea profesional, imparcial y transparente en su preparación y administración a lo largo de todo el ciclo electoral".¹⁴ Algunos¹⁵ miembros de la DoP han desarrollado metodologías de observación de un proceso electoral, incluido el uso de las e-TIC, basadas en estos principios.

A continuación se describen brevemente estos principios:

El voto secreto

El voto secreto está en el corazón de un proceso electoral democrático, y cualquier proceso de votación, recuento y tabulación que no cumpla con este compromiso verá reducida su credibilidad, dependiendo de la magnitud del incumplimiento. El voto secreto significa que no debe ser posible asociar un voto a un votante concreto, lo que permite al votante ejercer su elección libremente, sin posibilidad de coacción, intimidación o compra de votos.

Para los sistemas e-TIC asociados al censo electoral, el principio se aplica al tratamiento de los datos personales de los votantes, su privacidad y las medidas adoptadas para garantizar que sólo se utilizan para los fines prescritos por la ley.¹⁶ Privacy International ha identificado las siguientes condiciones de acceso a los datos contenidos en el registro de votantes basándose en los principios de protección de datos y las mejores prácticas:¹⁷ El registro de votantes no debe incluir más datos personales que los necesarios para establecer la elegibilidad para votar. La ley debe definir las normas mínimas de seguridad para proteger el registro de votantes contra el acceso no autorizado; también debe definir las condiciones y límites de acceso a los datos contenidos en el registro de votantes. Los datos personales del censo electoral no deberían ser públicos por defecto. Si va a haber un registro abierto al que cualquiera pueda comprar acceso para cualquier propósito, éste debería funcionar sobre una base de inclusión voluntaria (opt-in) en lugar de exclusión voluntaria (opt-out). Debería quedar claro en la legislación y en los lineamientos pertinentes que los datos personales del

¹⁴ Informe de la Comisión Global sobre Elecciones, Democracia y Seguridad (2012) "Profundizando la Democracia, una estrategia para mejorar la integridad de las elecciones en todo el mundo." https://storage.googleapis.com/kofiannanfoundation.org/2016/01/deepening_democracy_0.pdf

¹⁵ Consulte, por ejemplo, OSCE/ODIHR, Handbook for the observation of new voting technologies(2013). <https://www.osce.org/odihr/elections/104939?download=true>, Recomendaciones del Consejo de Europa sobre normas para el voto electrónico www.coe.int/en/web/electoral-assistance/e-voting Instituto Nacional Demócrata, Monitoreo de tecnologías electrónicas en procesos electorales (2007), https://www.ndi.org/sites/default/files/2267_elections_manuals_monitoringtech_0.pdf, Organización de los Estados Americanos, La Observación del Uso de las Tecnologías Electorales: Manual para las misiones de observación electoral de la OEA <https://www.oas.org/es/sap/docs/Technology%20English-FINAL-4-27-10.pdf>

¹⁶ En la UE (y el EEE) la protección de datos y la privacidad están reguladas por el Reglamento General de Protección de Datos (2016/679), que se aplica en el contexto de unas elecciones. Elementos adicionales específicos para las elecciones fueron añadidos por el Consejo Europeo de Protección de Datos antes de las recientes elecciones al Parlamento de la UE en 2019 (EDPB, Declaración 2/2019) y por el Consejo de Europa con el (2018), Convenio modernizado para la protección de las personas con respecto al tratamiento de datos personales.

¹⁷ Privacy International, Tecnología, datos y elecciones: Una lista del ciclo electoral, <https://privacyinternational.org/advocacy/3093/technology-data-and-elections-checklist-election-cycle>

censo electoral que se hayan hecho accesibles siguen estando sujetos a la legislación sobre protección de datos y protegidos por ella, incluso para su tratamiento sucesivo.

Debe regularse el acceso y la utilización de los datos personales contenidos en un censo electoral. Quién tiene derecho a acceder y con qué fines debe estar claramente estipulado en la ley, limitado a lo necesario para el proceso electoral, con prohibiciones claras de utilizar estos datos para cualquier otro fin.

Integridad del voto

El recuento exacto de los votos y la publicación de los resultados implican una cadena de acciones. Todos los votos deben emitirse según lo previsto y deben contabilizarse tal y como se emitieron, sin que se sumen o resten votos ilegalmente. Los votantes deben tener la certeza de que los votos se emiten y contabilizan sin modificaciones. La seguridad del sistema de gestión de resultados debe garantizar que no haya posibilidad de fraude o error no detectado que altere los resultados. En un proceso de votación en papel, la integridad de esta cadena puede garantizarse mediante la observación de cada paso del proceso¹⁸ y la verificación, si es necesario y lo permite la legislación, mediante la posibilidad de un recuento manual; las e-TIC están sujetas a los mismos requisitos.

Principio de igualdad del voto (una persona-un voto)

Significa que ningún votante puede emitir más votos que otro. Los sistemas de e-TIC deben impedir que cualquier persona emita más votos de los establecidos por la ley y deben impedir que se sustraigan votos del sistema. Algunos sistemas de voto electrónico permiten a los votantes emitir su voto más de una vez, con la condición de que sólo se contabilice el último voto emitido. Esto ayuda a reducir el riesgo de coacción del votante y de compra de votos. Por consiguiente, debe ser posible verificar que no se ha producido ninguna violación del principio de igualdad.

Universalidad del sufragio

Esto significa que todos los ciudadanos adultos con derecho a voto deben tener la oportunidad de votar y que se deben proporcionar medios efectivos para su participación.

Transparencia

Un proceso electoral transparente es aquel en el que cada paso está abierto al escrutinio de las partes interesadas (partidos políticos, observadores electorales, medios de comunicación, tribunales y votantes), que pueden verificar de forma independiente que el proceso se desarrolla de acuerdo con los procedimientos y sin irregularidades. Ofrecer transparencia en unas elecciones ayuda a establecer la confianza pública en el proceso, ya que los votantes disponen de un medio para verificar que los resultados reflejan fielmente la voluntad del pueblo. La Asamblea General de la ONU reiteró¹⁹ que "...la transparencia es una base

¹⁸ Aunque en algunos casos esto no es totalmente posible para todas las partes interesadas, por ejemplo en el caso del voto por correo, en el que la integridad depende de la seguridad y fiabilidad del servicio postal. Consulte, por ejemplo, Comisión de Venecia, "On the compatibility of remote voting and electronic voting with the Standards of the Council of Europe". [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2004\)012-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2004)012-e).

¹⁹ Resolución de las Naciones Unidas sobre el fortalecimiento de la función de las Naciones Unidas para promover la democratización y mejorar las elecciones periódicas y auténticas, (2019) A/RES/74/158. <https://digitallibrary.un.org/record/3847788?ln=en>

fundamental para que los gobiernos rindan cuentas a sus ciudadanos, lo que, a su vez, es un pilar de las sociedades democráticas".

El Consejo de Europa es hasta ahora la única²⁰ organización que ha adoptado normas intergubernamentales sobre el voto electrónico.²¹ La recomendación también incluye normas sobre transparencia y observación, dejando claro que "cualquier observador, en la medida en que lo permita la ley, deberá poder observar y comentar las elecciones electrónicas, incluida la compilación de los resultados".

Aplicado a los aspectos específicos del voto electrónico, el Consejo de Europa pidió en 2017 a los Estados miembros que fueran transparentes en todos los aspectos. "Se informará al público, en particular a los votantes, con suficiente antelación al inicio de la votación, en un lenguaje claro y sencillo, sobre: cualquier paso que un votante tenga que dar para participar y votar; el uso y funcionamiento correctos de un sistema de votación electrónica; el calendario de votación electrónica, incluidas todas las etapas." Además, "los componentes del sistema de voto electrónico se divulgarán a efectos de verificación y certificación".²²

Antes de introducir tecnologías, se deben consultar a las principales partes interesadas las razones por las que se proponen soluciones de e-TIC, cómo podrían abordar retos específicos y mejorar el proceso electoral, así como lo que no pueden lograr y sus riesgos asociados y los planes para mitigarlos. Estas cuestiones deben explicarse claramente a los medios de comunicación y a los ciudadanos observadores desde el principio del proceso de adopción de las e-TIC.²³ La transparencia del proceso de contratación es esencial para la rendición de cuentas, el consenso y la confianza. Los principales donantes deberían establecer criterios y recomendaciones claros, sobre todo teniendo en cuenta que la contratación pública está cubierta por la financiación destinada al apoyo a la democracia y al apoyo electoral.²⁴

²⁰ Estados Unidos ha adoptado las Directrices Voluntarias para el Sistema de Votación, un conjunto de especificaciones y requisitos con los que se pueden probar los sistemas de votación para determinar si cumplen las normas exigidas. <https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines>

²¹ La recomendación se adoptó el 14 de junio de 2017 y se complementa con las directrices sobre la aplicación de las disposiciones de la recomendación con requisitos específicos y la exposición de motivos. <https://www.coe.int/en/web/electoral-assistance/e-voting>

²² Recomendación Rec(2017)5 del Comité de Ministros a los Estados miembros sobre los estándares para el voto electrónico: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f

²³ Informe del Secretario General de las Naciones Unidas sobre la asistencia electoral de la ONU (2019) A/74/285, párr. 38. <https://dppa.un.org/sites/default/files/sg-electoral-assistance-report-final-20191114-e.pdf>

²⁴ Por ejemplo, las recomendaciones de la UE sobre contratación incluyen: "Verificar qué soluciones y licencias están ya disponibles para su reutilización. Solicitar funcionalidades que hagan efectiva la transferencia de datos. Solicitar soluciones TIC fácilmente accesibles para todos. Evitar hacer referencia a productos patentados como: nombres de marca, marcas registradas y patentes. No solicitar soluciones con funcionalidades que vayan más allá de lo necesario Evaluar el ejercicio de contratación pública". Consulte las directrices de la UE sobre contratación pública: <https://joinup.ec.europa.eu/collection/e-procurement/discussion/guidelines-procuring-it-solutions> Referencias adicionales a las decisiones de la Comisión Europea en el contexto de la contratación pública: "[Contra la dependencia: creación de sistemas de TIC abiertos mediante un mejor uso de las normas en la contratación pública, COM](#)" (2013) 455 final, p.4. (en inglés); "[Compartir y reutilizar" las cláusulas de los contratos, Cláusulas contractuales para la contratación de servicios, p.22. \(en](#)

También se recomienda que las partes interesadas nacionales, incluidos los candidatos, los medios de comunicación y la sociedad civil, tengan la oportunidad de realizar aportaciones significativas y de supervisar la selección y la aplicación de dichos sistemas.²⁵

Definir quién está mejor situado para promover, evaluar y verificar el principio de transparencia es una cuestión importante, y es una cuestión relacionada en cierta medida con el principio de responsabilidad. Aunque los candidatos y los observadores electorales tienen un papel fundamental que desempeñar en la promoción de la transparencia de un proceso electoral, corresponde en última instancia al OE garantizar el cumplimiento de este principio.

Los sistemas e-TIC con frecuencia requieren un cierto grado de experiencia para comprenderlos plenamente, sin embargo, el principio de transparencia exige que los sistemas e-TIC desplegados no impidan a las personas examinar y comprender los resultados electorales, incluso sin conocimientos técnicos especializados. En algunos países existen requisitos específicos sobre el cumplimiento de este principio, como ejemplifica la sentencia del tribunal federal alemán sobre el uso de máquinas de votación.²⁶ En opinión del tribunal, la transparencia sólo está garantizada si "los pasos esenciales de la votación y la tabulación de los resultados pueden examinarse de forma fiable y sin necesidad de conocimientos especializados en la materia."

Por lo tanto, es esencial que un OE fomente un entorno que garantice a todas las partes interesadas en el proceso electoral el acceso al mismo para llevar a cabo una observación significativa, ya sea directamente o a través de expertos técnicos.²⁷ Las directrices del Consejo de Europa que acompañan a su Recomendación, por ejemplo, dejan claro que "los observadores, incluidos los representantes de los partidos políticos y el público en general, deben tener acceso a toda la información pertinente durante todo el proceso de certificación para poder cumplir con su deber". Además, la exposición de motivos de la Recomendación hace hincapié en que "los observadores, en la medida en que lo permita la ley, deben poder verificar que el propio sistema de voto electrónico está diseñado y funciona de forma que

[\(inglés\) Directriz sobre la contratación pública de software de código abierto \(2010\), p.42, 56. \(en inglés\) "Guide for the procurement of standards-based ICT — Elements of Good Practice SWD" \(2013\)224 final, p.33.](#)

²⁵ DoP, párrafo 16, "Los ciudadanos tienen el derecho internacionalmente reconocido de asociarse y de participar en los asuntos gubernamentales y públicos de su país. Estos derechos pueden ejercerse a través de organizaciones no gubernamentales que supervisen todos los procesos relacionados con las elecciones y observen los procedimientos, incluido, entre otras cosas, el funcionamiento de las tecnologías electorales electrónicas y de otro tipo en el interior de centros de votación, centros de recuento y otras instalaciones electorales, así como el transporte de papeletas y otros materiales sensibles..."

²⁶ Sentencia del Tribunal Constitucional Federal alemán sobre el uso de máquinas de votación electrónica, 3 de marzo de 2009.
https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html.

²⁷ DoP, Párrafo 14, "Los contendientes políticos (partidos, candidatos y partidarios de posiciones en referendos) tienen intereses creados en el proceso electoral a través de sus derechos a ser elegidos y a participar directamente en el gobierno. Por lo tanto, se les debe permitir supervisar todos los procesos relacionados con las elecciones y observar los procedimientos, incluido, entre otras cosas, el funcionamiento de las tecnologías electorales electrónicas y de otro tipo en el interior de centros de votación, centros de recuento y otras instalaciones electorales, así como el transporte de papeletas y otros materiales sensibles."

respetar los principios fundamentales de las elecciones y referendos democráticos. Por lo tanto, los Estados deben tener disposiciones legales claras sobre el acceso de los observadores a la documentación del sistema de voto electrónico y a los datos de auditoría".²⁸

Es importante señalar también en este sentido que la propiedad intelectual o el secreto comercial no deben utilizarse como justificación para obstaculizar los principios de transparencia. Este es un problema recurrente cuando se emplean soluciones digitales para la prestación de servicios públicos y cada vez se reconoce más la necesidad de establecer medidas de seguridad para limitar la capacidad de empresas y gobiernos de utilizar la propiedad intelectual o el secreto comercial como forma de protegerse del escrutinio.

Las e-TIC implican una serie de otras actividades, algunas críticas para la integridad del proceso, que pueden observarse pero que tienen lugar mucho antes del día de las elecciones. Entre ellas se incluyen las pruebas y la certificación de los sistemas y la instalación del software. Cualquier proceso de verificación/auditoría debe estar dirigido por actores nacionales y guiado por expertos independientes seleccionados en un proceso inclusivo y transparente. Los OE deben garantizar la transparencia facilitando información sobre las pruebas y la certificación de los sistemas de e-TIC, algo que se establece claramente en la DoP: "[El OE] garantiza el acceso sin obstáculos de la misión de observación electoral internacional a todas las fases del proceso electoral y a todas las tecnologías electorales, incluidas las tecnologías electrónicas y los procesos de certificación del voto electrónico y otras tecnologías, sin exigir a las misiones de observación electoral que suscriban acuerdos de confidencialidad u otros acuerdos de no divulgación relativos a las tecnologías o los procesos electorales, y reconoce que las misiones de observación electoral internacional pueden no certificar las tecnologías como aceptables...".²⁹ Por último, en el contexto de la transparencia, la adopción de un enfoque de datos electorales abiertos es una buena práctica que garantizaría un mayor nivel de transparencia y acceso a todas las partes interesadas, fortificando en gran medida la confianza en el proceso electoral.

Rendición de cuentas

Las elecciones son el principal medio por el que los votantes exigen responsabilidades a los elegidos. También debe haber rendición de cuentas en un proceso electoral para que sea auténtico y refleje la voluntad del pueblo.

Los OE son el centro del principio de rendición de cuentas para el proceso electoral, incluidos los sistemas de e-TIC. Sin embargo, la rendición de cuentas se extiende también a los proveedores, los organismos de certificación y otros implicados en la adquisición, la gestión y el uso. Los funcionarios electorales deben ser responsables del desarrollo general de las elecciones, incluida la supervisión de las e-TIC. Si las e-TIC incluyen tecnología suministrada por proveedores privados, las funciones y responsabilidades de estos proveedores deben estar claramente definidas, así como los mecanismos adecuados y claros para su gestión y supervisión. Del mismo modo, las agencias de certificación y otros organismos deben rendir cuentas estrictamente para garantizar que cumplen con sus respectivas responsabilidades.

²⁸ Exposición de motivos de la Recomendación CM/Rec(2017)5 del Consejo de Europa. Párrafo 98.

²⁹ DoP, párrafo 12(b).

Aplicar el principio de rendición de cuentas a las elecciones que utilizan sistemas de e-TIC puede resultar complicado. En primer lugar, para determinar las consecuencias de algunas acciones llevadas a cabo por los funcionarios puede ser necesario enfrentarse a una falta de transparencia, ya que pueden no ser visibles (puesto que tienen lugar dentro de una máquina) o no entenderse bien, por lo que establecer la rendición de cuentas se hace más complicado. En segundo lugar, muchos aspectos de la aplicación de los sistemas de e-TIC exigen que los OE dispongan de personal altamente capacitado y de una conciencia institucional de los principios de las TIC. En tercer lugar, dadas estas consideraciones y la naturaleza técnica del proceso, es habitual que los proveedores comerciales ayuden al OE, llegando en algunos casos casi a asumir algunas de sus responsabilidades, lo que va en contra del principio de que el OE es el único responsable de todo el proceso.

Los OE deben esforzarse por aumentar su propia responsabilidad. Es especialmente importante que cada acción emprendida quede debidamente registrada por el sistema y sea verificable. El proceso de adquisición y adopción de nuevas soluciones de e-TIC debe ser integrador y transparente. Esto es especialmente necesario en una situación en la que se implementan nuevas tecnologías que pueden no ser ampliamente comprendidas por el público o los contendientes electorales. Los organismos de gestión electoral también pueden permitir que los partidos políticos, los observadores electorales y los medios de comunicación asistan a las reuniones en las que se formulan las políticas, especialmente en lo que respecta a la introducción y el uso de nuevas tecnologías. Las auditorías postelectorales y los ejercicios de "lecciones aprendidas" también contribuyen a fomentar un sentimiento de apropiación del proceso por parte de los actores electorales.

Los OE deben mantener el control de la relación con el proveedor y asegurarse de que ésta no vulnera su propia soberanía sobre el proceso electoral. Esto se aplica especialmente al tratamiento de los datos recogidos y almacenados, que pertenecen al Estado y están sujetos a las leyes y requisitos del país y sometidos a la jurisdicción del sistema judicial nacional. En unas elecciones en las que determinadas fases del proceso se contratan a terceros, el OE sigue siendo el responsable general. El papel del proveedor debe definirse claramente para que el OE conserve el control del proceso en todo momento; más concretamente, el OE debe seguir siendo el responsable del tratamiento de los datos, determinando la finalidad y los medios del tratamiento de los datos personales. Deben evitarse las situaciones de dependencia de un solo proveedor, en las que el OE no puede cambiar fácilmente de proveedor porque no dispone de toda la información esencial sobre el sistema para que un proveedor alternativo pueda hacerse cargo de él.³⁰ Es responsabilidad de los funcionarios electorales garantizar que el proceso cumpla los plazos y los requisitos legales, y colaborar estrechamente con los proveedores para asegurarse de que se cumplen estos criterios.

Seguridad digital

El creciente uso de los sistemas TIC en todo el mundo y su vulnerabilidad a la manipulación malintencionada por parte de agentes tanto nacionales como extranjeros ha hecho de la

³⁰ Decisiones de la Comisión Europea en un contexto de contratación pública: ["Contra la dependencia: creación de sistemas de TIC abiertos mediante un mejor uso de las normas en la contratación pública, COM" \(2013\) 455 final, p.4. \(en inglés\)](#); ["Compartir y reutilizar" las cláusulas de los contratos, Cláusulas contractuales para la contratación de servicios, p.22. \(en inglés\)](#) [Directriz sobre la contratación pública de software de código abierto \(2010\), p.42, 56. \(en inglés\)](#) [Guía para la adquisición de TIC basadas en estándares - Elementos de buenas prácticas SWD \(2013\)224 final, p.33. \(en inglés\)](#)

ciberseguridad uno de los factores cruciales para preservar la confianza pública, especialmente en el contexto de las e-TIC, por lo que en los últimos años se ha asistido a un aumento de la concienciación y la acción para hacer que los sistemas e-TIC sean más seguros y menos susceptibles de manipulación supuesta o real.

La protección de los equipos y programas informáticos de registro y emisión de votos es esencial para la integridad de las elecciones. Existe un vasto y descentralizado ecosistema de tecnologías que apoyan las elecciones, incluidos los sistemas de registro de votantes en línea, los sistemas de conteo de votantes y los sistemas de auditoría. Todas estas tecnologías son susceptibles de ataques digitales y errores internos, que pueden afectar a la confianza de los votantes y a la integridad de las elecciones.³¹

El Panel de Alto Nivel sobre Cooperación Digital del Secretario General de la ONU hace de la confianza, la seguridad y la estabilidad digitales una de las principales áreas de cooperación multilateral para "dar forma a una visión compartida, identificar los atributos de la estabilidad digital, dilucidar y reforzar la aplicación de normas para el uso responsable de la tecnología y proponer prioridades de actuación". Pide un Compromiso Mundial sobre Confianza y Seguridad Digitales multilateral para reforzar los esfuerzos³² existentes en este sentido. Otro ámbito de actuación clave es profundizar en la cooperación y el intercambio de información entre los Equipos de Respuesta ante Emergencias Informáticas (CERT) nacionales. Estas iniciativas no sólo incluyen a los Estados miembros y las organizaciones regionales, sino también al sector privado.

En este contexto, cabe señalar una serie de iniciativas, tanto a escala mundial como regional. En términos de ciberseguridad más amplia y cooperación internacional en torno a asegurar la integridad electoral, vale la pena mencionar la cooperación que se ha desarrollado en torno a la iniciativa Llamado de París para la Confianza y la Seguridad en el Ciberespacio,³³ lanzada en 2018, que específicamente llama a fortalecer las capacidades para prevenir la interferencia maligna de actores extranjeros destinada a socavar los procesos electorales a través de actividades cibernéticas maliciosas³⁴. A nivel regional, el Grupo de Cooperación en materia de Redes y Sistemas de Información (NIS) de la UE publicó en 2018 las directrices del "Compendio sobre seguridad cibernética de la tecnología electoral" (en inglés).³⁵ El

³¹ Informe de la Comisión Kofi Annan sobre las elecciones y la democracia en la era digital, enero de 2020: https://www.kofiannanfoundation.org/app/uploads/2020/01/f035dd8e-kaf_kacedda_report_2019_web.pdf

³² El Grupo de Expertos Gubernamentales (GEG) de las Naciones Unidas sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional, creado en 1998, propuso once normas voluntarias y no vinculantes para los Estados miembros, que fueron acogidas favorablemente por la Asamblea General de las Naciones Unidas en 2015.

³³ La convocatoria de París se lanzó en 2018 y a ella se sumaron 65 países y 334 empresas, entre ellas las principales tecnológicas mundiales y 138 universidades y ONG. Muchas de las principales potencias tecnológicas, como Estados Unidos, Rusia, China, Israel e India, aún no se han sumado a la iniciativa. <https://pariscall.international/en/principles>

³⁴ Una iniciativa interesante para abordar la vulnerabilidad a los ciberataques de los partidos políticos y los candidatos fue la promovida por el NDI (Instituto Nacional Demócrata) y el IRI (International Republican Institute) que, junto con el Harvard Belfer Centre y su proyecto Defending Digital Democracy, han elaborado "manuales de procedimientos" prácticos para casos concretos. <https://www.belfercenter.org/D3P#!playbooks>

³⁵ http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53645

Comité del Convenio sobre la Ciberdelincuencia del Consejo de Europa también ha elaborado una breve nota orientativa³⁶ sobre la aplicación de sus disposiciones a los delitos electorales. La Guía de Commonwealth sobre Ciberseguridad Electoral describe principios para la ciberseguridad electoral,³⁷ así como recomendaciones organizativas específicas que pueden ser adaptadas por los OE,³⁸ junto con material técnico que puede ayudar con retos específicos. También se pueden encontrar recomendaciones similares en el Proceso Holístico de Pruebas de Exposición y Adaptación (HEAT) de IFES de 2018.³⁹ Del mismo modo, reconociendo que la cooperación interinstitucional es necesaria para fortalecer la ciberseguridad de un proceso electoral, el Instituto Internacional para la Democracia y la Asistencia Electoral (IDEA) publicó en 2019 "Ciberseguridad en las elecciones - modelos de colaboración interinstitucional,"⁴⁰ en el que se describen varios modelos de dicha cooperación. Recomienda, entre otras cosas, la transparencia como principio esencial para preservar la independencia del OE, al tiempo que establece la cooperación con otros organismos gubernamentales en los esfuerzos por lograr la seguridad del sistema, la participación del sector privado, el mundo académico, los medios de comunicación y la sociedad civil, la cooperación internacional y la designación de las elecciones como infraestructura crítica como medida para fomentar la colaboración entre organismos.

Responsabilidades de las partes interesadas [y rendición de cuentas]

Este capítulo está dedicado a aclarar las diferentes responsabilidades que las partes interesadas, tanto nacionales como internacionales, tienen en el proceso de selección, adquisición y utilización de las e-TIC en el proceso electoral. Las orientaciones sobre este proceso, o partes seleccionadas del mismo, están disponibles en publicaciones⁴¹ de diversas organizaciones internacionales.

³⁶ Aspectos de la interferencia electoral mediante sistemas informáticos cubiertos por el Convenio de Budapest, adoptado el 8 de julio de 2019: <https://rm.coe.int/t-cy-2019-4-guidance-note-election-interference/1680965e23>

³⁷ [https://thecommonwealth.org/sites/default/files/inline/Cybersecurity for Elections PDF 0.pdf](https://thecommonwealth.org/sites/default/files/inline/Cybersecurity%20for%20Elections%20PDF%200.pdf)

³⁸ También se pueden encontrar recomendaciones similares en IFES: Desarrollo de un proceso holístico de pruebas de exposición y adaptación (HEAT) para los organismos de gestión electoral. <https://www.ifes.org/publications/cybersecurity-elections>

³⁹ <https://www.ifes.org/publications/cybersecurity-elections>

⁴⁰ <https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf>

⁴¹ Proyecto ACE, elecciones y tecnología. <https://aceproject.org/ace-en/topics/et/onePage>
Consejo de Europa, recomendación (2017)5 sobre el voto electrónico.

https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f

Comisión Europea, "Guía para la contratación de TIC basadas en normas - Elementos de buenas prácticas" (en inglés). https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2326

Grupo de trabajo conjunto UE-PNUD, "Aspectos de la contratación pública en la introducción de soluciones TIC en los procesos electorales": El caso específico del censo electoral (2010) (en inglés) <http://aceproject.org/ero-en/misc/procurement-aspects-of-introducing-icts-solutions>;

IDEA, Introducción del voto electrónico: consideraciones esenciales. (en inglés)

<https://www.idea.int/es/publications/catalogue/introducing-electronic-voting-essential-considerations> .

IDEA, Introducción de la tecnología biométrica en las elecciones, (2017), (en inglés)

<https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>

El Organismo Electoral (OE)

El OE es responsable de todo el proceso electoral, incluidos todos los aspectos del proceso de adopción, adquisición, despliegue y utilización de soluciones de e-TIC. Junto con el parlamento nacional, el OE debe ser el órgano responsable de facilitar la reflexión y el debate que puedan conducir a la adopción de las e-TIC mediante el establecimiento de amplias consultas con los actores políticos y la sociedad civil con el fin de llegar a una decisión basada en hechos que tenga en cuenta el espectro de opiniones más amplio posible.

Es importante señalar que, si se aplica de acuerdo con las buenas prácticas, el proceso de adopción puede llevar bastante tiempo, por lo que el OE debe considerar adecuadamente su calendario en relación con el ciclo electoral. Una aplicación precipitada dará lugar inevitablemente a que algunas partes del proceso no se apliquen plenamente, con posibles repercusiones negativas en la calidad del resultado y en la confianza que las partes interesadas tendrán en las e-TIC. El calendario de introducción de las e-TIC debe incluir el tiempo adecuado para realizar un estudio de viabilidad y para los pilotos y pruebas de las nuevas e-TIC. Además, una vez aprobado el proyecto, las autoridades nacionales deberán financiarlo oportuna y adecuadamente.

A lo largo del proceso, otra tarea clave del OE es garantizar la transparencia del proceso, un factor importante para aumentar la confianza de las partes interesadas, lo que incluye tanto dar un acceso significativo a la documentación pertinente a las partes interesadas y los observadores como mantener informado al público a través de programas de información a los votantes.

Cuando esté en juego la integridad de una infraestructura crítica,⁴² deberán aplicarse requisitos y procedimientos de control estrictos a la implementación de las e-TIC, prestando especial atención a su integridad y seguridad. En los casos en que, por diversas razones, el OE no pueda reunir los conocimientos técnicos necesarios para dirigir todo este proceso, deberá requerirse el apoyo de expertos, ya sea por parte de agentes nacionales o de fuentes externas, y deberá exigirse a los proveedores comerciales que extremen la diligencia debida en sus prácticas.

IFES, Tecnologías de votación y recuento electrónicos: Guía para la realización de estudios de viabilidad (2011), (en inglés)

https://www.ifes.org/sites/default/files/electronic_voting_and_counting_tech_goldsmith_0.pdf

IFES y NDI, Implementación y supervisión de las tecnologías de votación y recuento electrónicos (2013) (en inglés),

https://www.ifes.org/sites/default/files/implementing_and_overseeing_electronic_voting_and_counting_technologies_0.pdf

⁴² Infraestructura crítica se refiere a los sistemas y activos cuya "incapacidad o destrucción... tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la salud pública nacional o la seguridad, o cualquier combinación". El Departamento de Seguridad Nacional de Estados Unidos designó los sistemas y activos utilizados para administrar las elecciones como subsector de infraestructuras críticas en 2017. Esto incluye las ubicaciones físicas (instalaciones de almacenamiento, colegios electorales y lugares donde se tabulan los votos) y la infraestructura tecnológica (bases de datos de registro de votantes, sistemas de votación y otra tecnología utilizada para gestionar las elecciones e informar y validar los resultados). No incluye la infraestructura relacionada con las campañas políticas. En la UE, la Agencia de Ciberseguridad ENISA propuso la misma designación ante las elecciones al Parlamento Europeo de 2019.

Con el eventual apoyo técnico de **organismos especializados** (como las agencias de ciberseguridad y protección de datos) y **otros expertos externos**, el OE debería dirigir la fase crucialmente importante de definición de las especificaciones técnicas de las soluciones e-TIC que el país haya decidido adoptar, y asegurarse de que los principios fundamentales para las elecciones descritos en la primera parte de este documento sean garantizados por las e-TIC previstas. Si se dispone de los conocimientos técnicos necesarios, también debería abarcar la fase de estudio de viabilidad, pilotaje, pruebas, certificación del sistema y auditorías periódicas posteriores; de lo contrario, habrá que buscarlos en el extranjero.

Si bien el OE puede ser responsabilizado por una serie de instituciones y partes interesadas, la rendición de cuentas del OE debe ser reforzada por un poder **judicial** fuerte e independiente, que suele desempeñar un papel clave en la resolución de litigios, al menos en última instancia, incluidos los relacionados con las TIC electorales. Un problema común de rendición de cuentas en el contexto de los sistemas digitales, incluidas las e-TIC, es la falta de mecanismos de recurso colectivo, que permitan a las organizaciones presentar reclamaciones en nombre de un número indeterminado de personas que se hayan visto afectadas negativamente. En el caso concreto del OE, el papel del poder judicial también puede complementarse con requisitos legales de información pública sobre las reclamaciones presentadas ante los OE, lo que añadiría un nivel adicional de transparencia a su labor.

En la probable situación de que esto no pueda desarrollarse internamente y haya que externalizarlo, el OE tiene también la responsabilidad general de la fase clave de licitación y contratación de las e-TIC, actuando dentro del marco nacional de contratación pública (que debe basarse en la transparencia, la competencia y criterios objetivos en la toma de decisiones) y de eventuales marcos anticorrupción relacionados con la contratación.

La contratación pública debe gestionarse teniendo en cuenta el calendario electoral, pues de lo contrario se corre el riesgo de que las licitaciones se adjudiquen precipitadamente, con decisiones poco transparentes y sin incluir en los contratos cuestiones clave. Las adquisiciones realizadas de forma precipitada y con adjudicación directa (contrato de proveedor único) normalmente deberían alertar a los organismos nacionales de control y no contribuyen a la confianza pública en los sistemas adoptados. Cuando el OE no puede contar con conocimientos técnicos profesionales, a veces confía ciegamente en los proveedores comerciales. Todas estas prácticas tienen importantes repercusiones negativas en la confianza general de las partes interesadas en las e-TIC y también podrían dar lugar a una solución que no funcione según lo previsto, comprometiendo potencialmente la integridad y la credibilidad de todo el proceso electoral.

Los principales textos internacionales sobre contratación pública⁴³ hacen hincapié en la importancia de la transparencia de la contratación y de la información pública como forma

⁴³ Los Principios de la OCDE para la Integridad en la Contratación Pública, destacan los dos principios clave que sustentan la transparencia en la contratación pública, a) Proporcionar un grado adecuado de transparencia en todo el ciclo de contratación con el fin de promover un trato justo y equitativo para los proveedores potenciales, b) Maximizar la transparencia en la licitación competitiva y tomar medidas cautelares para mejorar la integridad, en particular para las excepciones a la licitación competitiva. <https://www.oecd.org/gov/ethics/48994520.pdf>

Los Art. 9 y 10 de la Convención de las Naciones Unidas contra la corrupción también destacan aspectos importantes de la transparencia y la información pública en un proceso de contratación

de reforzar la confianza de las partes interesadas en el proceso. Para las partes interesadas nacionales, tener acceso sin obstáculos a la documentación pertinente es una condición previa fundamental para desempeñar sus funciones de manera significativa. El papel de los observadores internacionales, además de buscar información sobre el sistema y analizarla, debe centrarse también en evaluar si se ha concedido adecuadamente este derecho a las partes interesadas nacionales.

Una vez adjudicada la licitación de e-TIC, el OE debe seguir ejerciendo su responsabilidad y supervisar la ejecución del contrato con el proveedor. En este caso, el OE debe supervisar la aplicación y el vendedor no debe poder tomar ninguna medida que afecte a la funcionalidad del equipo sin la autorización del organismo de gestión electoral. Para el OE es importante que el proceso de adquisición dé lugar a requisitos contractuales que incluyan plazos de entrega firmes que se correspondan con el calendario electoral, y tiempo suficiente para realizar auditorías de los equipos y corregir las deficiencias en el rendimiento del proveedor, así como sanciones suficientes para disuadir del incumplimiento.

Los OE también deben asegurarse de que las soluciones e-TIC sean probadas y certificadas por una **autoridad independiente** antes de ser aprobadas para su uso. Pueden realizarse auditorías a intervalos regulares para verificar que el equipo en uso es el mismo que el certificado. Es importante subrayar también que la certificación de las soluciones e-TIC no es competencia de los observadores internacionales.

Por último, aunque los OE tienen una responsabilidad especial a la hora de valorar los pros y los contras de la introducción de las e-TIC, es fundamental que el proceso electoral siga perteneciendo a los ciudadanos, en cuya voluntad se basa la autoridad del gobierno.

Otras partes interesadas nacionales

Las partes interesadas nacionales, los partidos políticos, la sociedad civil (incluidos los observadores electorales) y los medios de comunicación tienen un papel importante que desempeñar en las primeras deliberaciones sobre la adopción de las e-TIC participando en los debates iniciales. Después de esto, todos los actores electorales tienen la responsabilidad crucial de hacer que los OE rindan cuentas supervisando sus actividades y señalando cualquier violación a la atención del poder judicial y del público. Debido a la naturaleza técnica de los sistemas de e-TIC, las partes interesadas pueden necesitar desarrollar habilidades específicas para hacer aportaciones significativas a las deliberaciones, y especialmente los medios de comunicación tienen la responsabilidad de desarrollar una comprensión adecuada de los sistemas en uso en la medida necesaria para informar con precisión. La comprensión de los sistemas permitirá a las partes interesadas nacionales detectar infracciones y reunir las pruebas necesarias para presentar una denuncia.

En este contexto, también es vital que los partidos políticos participen de forma proactiva y responsable en el debate y en el posible proceso de adopción de las e-TIC e informen de forma proactiva a sus simpatizantes sobre lo que un nuevo sistema pretende aportar a las elecciones. Si todos los contendientes están igualmente informados y de acuerdo sobre la solución técnica y hay transparencia en el proceso global, no debería haber motivo para

pública. https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf

acusaciones no especificadas de manipulación de los resultados electorales a través de un sistema de e-TIC.

Como ya se ha mencionado, en las fases más técnicas se pueden poner a disposición del OE los conocimientos de **agencias nacionales especializadas** (agencias de ciberseguridad y protección de datos) o de **otros expertos externos** para garantizar que se alcance el objetivo común de obtener la mejor solución posible.

Fabricantes y vendedores de E-TIC

Las preocupaciones de los fabricantes y vendedores de tecnología electoral son diferentes de las de los funcionarios electorales. Su principal objetivo es obtener beneficios cumpliendo el contrato firmado con el OE.

Los fabricantes y proveedores tienen el deber de respetar los códigos de prácticas comerciales⁴⁴ u otros marcos reglamentarios aplicables. Además, dada la importancia crítica de los sistemas electorales en la vida democrática de un país,⁴⁵ deben aplicarse **requisitos más estrictos de debida diligencia**. Dado que la debida diligencia debe ser proporcional al riesgo y adecuada a las circunstancias y al contexto de una empresa específica, el grado de debida diligencia ejercido en el diseño de un sistema e-TIC debe ser similar al utilizado para garantizar la integridad de una infraestructura crítica. Esto tiene claras implicaciones también para las fases de conceptualización, diseño y prueba de nuevos productos TIC, así como para los conjuntos de datos y algoritmos subyacentes que los sustentan. Todo ello debe estar sujeto a una debida diligencia proactiva en materia de derechos humanos.⁴⁶

Como señalan los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos (UNGP): "la debida diligencia en materia de derechos humanos debe iniciarse lo antes posible en el desarrollo de una nueva actividad o relación, dado que los riesgos para los derechos humanos pueden incrementarse o mitigarse ya en la fase de estructuración de los contratos u otros acuerdos". La debida diligencia en materia de derechos humanos puede incluirse en sistemas más amplios de gestión del riesgo

⁴⁴ Por ejemplo, la OCDE publicó en 2018 directrices para una conducta empresarial responsable, con el objetivo de ayudar a las empresas a evitar y abordar los impactos adversos relacionados con los trabajadores, los derechos humanos, el medio ambiente, el soborno, los consumidores y el gobierno corporativo que puedan estar asociados con sus operaciones, cadenas de suministro y otras relaciones comerciales. <https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf>

⁴⁵ El concepto de debida diligencia en materia de derechos humanos es una parte fundamental del cumplimiento de la "responsabilidad empresarial de respetar", tal y como se define en los UNGP. La debida diligencia en materia de derechos humanos se refiere a los procesos que todas las empresas deben emprender para identificar, prevenir, mitigar y dar cuenta de cómo abordan los impactos potenciales y reales sobre los derechos humanos causados por sus propias actividades, o a los que contribuyen a través de ellas, o directamente vinculados a sus operaciones, productos o servicios por sus relaciones comerciales. también se está desarrollando en el contexto de la redacción del Tratado de la ONU sobre Empresas y Derechos Humanos, <https://www.business-humanrights.org/en/un-treaty-on-business-human-rights-negotiations-day-1-the-round-of-discussions-kicks-off-with-an-improved-draft>.

⁴⁶ Proyecto B-Tech de la OACDH Panorama general y alcance. https://www.ohchr.org/Documents/Issues/Business/BTech/B_Tech_Project_revised_scoping_final.pdf.

empresarial, siempre que vaya más allá de la mera identificación y gestión de los riesgos materiales para la propia empresa e incluya los riesgos para los titulares de derechos. Las directrices también sugieren que las empresas "traten el riesgo de causar o contribuir a abusos de los derechos humanos como una cuestión de cumplimiento legal dondequiera que operen".⁴⁷ En cuanto a la debida diligencia de las empresas en materia de derechos humanos, se está trabajando para ir más allá de los UNGP.⁴⁸ En 2014, la UE publicó una guía del sector de las TIC sobre la aplicación de los principios rectores.⁴⁹ Varios gobiernos han introducido recientemente, o han anunciado su intención de considerar la introducción de, regímenes legislativos para alentar o exigir a las empresas y grupos empresariales que lleven a cabo la debida diligencia obligatoria en materia de derechos humanos.⁵⁰

Algunos principios fundamentales pueden integrarse en el diseño de un sistema, lo que hace aún más probable que se respeten cuando el sistema esté en funcionamiento. Es importante, por tanto, que los proveedores comerciales también consideren estos principios como su objetivo final a la hora de plantearse la producción de nuevos sistemas de e-TIC.

Donantes internacionales y proveedores de asistencia técnica

Los donantes internacionales y los proveedores de asistencia técnica también tienen su parte de responsabilidad. En ocasiones, los donantes financian sistemas de e-TIC sobre todo como parte de sus programas de apoyo a la democracia y asistencia electoral, por lo que deben garantizar que la introducción de nuevas tecnologías respeta los principios democráticos y promueve los derechos humanos. Su principal responsabilidad es para con los beneficiarios, por lo que resulta aún más importante apoyar al OE en situaciones en las que no dispone de las competencias y los conocimientos necesarios para evaluar y decidir adecuadamente sobre la adquisición de e-TIC.

⁴⁷ Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos, punto 23(c), P.25.

⁴⁸ En el contexto de la Hoja de ruta para la cooperación digital de las Naciones Unidas, el Panel de Alto Nivel de las Naciones Unidas está estudiando el modo en que la comunidad internacional puede colaborar para optimizar el uso de las tecnologías digitales y mitigar los riesgos en el marco de alcanzar los Objetivos de Desarrollo Sostenible. Más concretamente sobre las tecnologías digitales y los derechos humanos, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos va a elaborar orientaciones para todo el sistema sobre la debida diligencia en materia de derechos humanos y las evaluaciones de impacto en el uso de las nuevas tecnologías en el marco del proyecto B-Tech iniciado en 2019.

https://www.un.org/en/content/digitalcooperationroadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf;

<https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx>.

⁴⁹ La UE también ha publicado orientaciones sectoriales para las empresas de TIC sobre cómo aplicar los principios rectores de la ONU. <https://op.europa.eu/en/publication-detail/-/publication/ab151420-d60a-40a7-b264-adce304e138b/language-en>.

⁵⁰ Estas propuestas parecen recibir un impulso especial en algunos Estados miembros de la Unión Europea y del Espacio Económico Europeo, así como en las instituciones de la UE. Documento de la ONU sobre propuestas legislativas para la debida diligencia obligatoria en materia de derechos humanos por parte de las empresas

https://www.ohchr.org/Documents/Issues/Business/MandatoryHR_Due_Diligence_Issues_Paper.pdf

El primer deber de los donantes debe ser ayudar a cerrar la brecha de capacitación y no dejar que el OE decida en la oscuridad. En tal situación, se deben responder preguntas importantes sobre la sostenibilidad del proyecto, ya que el OE podría carecer de las capacidades necesarias también para seguir la aplicación de la solución y su gestión y mantenimiento. Los proveedores de apoyo electoral deberían impartir, de manera responsable y constructiva, conocimientos especializados para ayudar y acompañar al OE en su proceso de toma de decisiones, así como en las pruebas y la introducción de las e-TIC y la formación de las partes interesadas nacionales para que puedan desempeñar su papel a la hora de garantizar la responsabilidad del OE durante el proceso.

En caso de que los donantes decidan apoyar al OE en la adopción de las e-TIC, deben asegurarse de que la adopción se basa en un análisis inclusivo para identificar la tecnología más eficaz para responder a los retos identificados conjuntamente y al contexto socioeconómico dado. Apoyar una evaluación exhaustiva de la viabilidad, incluidos el riesgo, el costo y la evaluación de la sostenibilidad en un proceso inclusivo antes de cualquier decisión de proceder debe ser la práctica habitual. La adquisición de soluciones tecnológicas debe hacerse de acuerdo con las leyes nacionales y las normas internacionales, con total transparencia, y debe ir seguida de la adopción y prueba del sistema e-TIC, así como de su introducción gradual, la formación de las partes interesadas y la educación efectiva de los votantes.⁵¹

Tras considerar las importantes cuestiones de necesidad, sostenibilidad y eficacia de un sistema de e-TIC propuesto, que seguirá siendo una decisión soberana del OE y de las partes interesadas nacionales, los donantes sólo deben promover soluciones que sean compatibles con los principios fundamentales de unas elecciones democráticas, la debida diligencia y el diseño ético.⁵² Éstas deben ofrecer garantías sólidas en términos de funcionalidad, seguridad y de preservación de la soberanía del OE sobre el proceso electoral.

También debe tenerse en cuenta la posible compatibilidad con las iniciativas destinadas a garantizar la transparencia de los sistemas de gobernanza, los códigos de buenas prácticas y otras iniciativas que se esfuerzan por promover la transparencia, como la iniciativa de Datos Abiertos.⁵³ Esta iniciativa también se ha adaptado para atender a las elecciones a través de la Iniciativa de Datos Electorales Abiertos,⁵⁴ lanzada por el Instituto Nacional Demócrata (NDI, por sus siglas en inglés), que establece principios y módulos de formación para los OE, observadores y otros. Esto debería contribuir a que la próxima generación de e-TIC garantice mejor los principios fundamentales para unas elecciones creíbles. Los datos abiertos son cruciales para la integridad electoral en la era digital y son esenciales para la confianza pública en las elecciones. Puede ayudar a mejorar el flujo de información dentro de los gobiernos y entre ellos, y a hacer más transparentes las decisiones y los procesos

⁵¹ En los casos en que un donante específico, por ejemplo la UE, financie la contratación, deberán tenerse en cuenta consideraciones específicas adicionales relacionadas con el donante, por ejemplo que se incluyan en la contratación las normas de la UE sobre identidad electrónica, ciberseguridad y protección de datos.

⁵² G. van Oortmerssen, "Ética y TIC: Más Allá del Diseño," Simposio Internacional de la IEEE sobre la Ética en Ciencias, Tecnología e Ingeniería, 2014 pp. 1-6, doi: 10.1109/ETHICS.2014.6893400.

⁵³ Los seis principios de la Carta fueron elaborados en 2015 por gobiernos, sociedad civil y expertos de todo el mundo para representar un conjunto de normas acordadas a nivel mundial sobre cómo publicar datos. <https://opendatacharter.net/principles/>.

⁵⁴ <https://openelectiondata.net/en/>

gubernamentales. Una mayor transparencia fomenta la rendición de cuentas y la buena gobernanza, mejora el debate público, ayuda a combatir la corrupción y, en última instancia, aumenta la credibilidad del proceso electoral.

Resumen

A continuación se exponen algunas condiciones no exhaustivas necesarias para que las e-TIC fomenten la integridad del proceso electoral y la confianza del público en el mismo:

Principios generales:

- a) Los sistemas de e-TIC deben seguir los principios fundamentales para unas elecciones democráticas, incluida la garantía de la integridad, el voto secreto, la universalidad y la igualdad del voto, la transparencia, la rendición de cuentas, la seguridad digital y la confianza pública. Los principios fundamentales para unas elecciones auténticas deben tenerse en cuenta y aplicarse en el diseño de un sistema de TIC, lo que hará aún más probable que los principios se respeten cuando el sistema esté en funcionamiento.
- b) Un marco jurídico y operativo debería complementar los sistemas e-TIC, proporcionando una base sólida para que se garanticen los principios fundamentales para unas elecciones democráticas, incluidos los procesos que proporcionan la transparencia y la rendición de cuentas necesarias para su adopción y uso, así como para su seguridad.
- c) La introducción y aplicación de los sistemas e-TIC debe adoptar un enfoque integrador, que implique a un amplio espectro de partes interesadas a lo largo de todo el proceso, para promover la transparencia y la confianza pública.
- d) La adopción de las e-TIC debe basarse en un análisis lo más integrador posible con las partes interesadas nacionales, a fin de identificar la solución más eficaz para responder a los retos identificados conjuntamente y al contexto socioeconómico dado. Debe ir precedida de una evaluación exhaustiva de la viabilidad, que incluya una evaluación de los riesgos, los costos y la sostenibilidad.
- e) La adquisición de e-TIC debe hacerse de acuerdo con las leyes nacionales y las normas internacionales, con total transparencia, y debe ir seguida de la adopción y prueba del sistema e-TIC, así como de su introducción gradual, la capacitación de las partes interesadas y la educación efectiva de los votantes.
- f) Posible punto sobre verificabilidad y rastro documental, además de auditorías definidas legalmente (IFES).
- g) La observación electoral es un aspecto clave de la transparencia y los observadores deben tener acceso a todos los documentos y la oportunidad de observar todas las fases del proceso electoral.

El OE:

- h) Los OE son responsables de todo el proceso electoral, incluidos todos los aspectos del proceso de adopción, adquisición y funcionamiento de las soluciones de e-TIC.
- i) Los OE deben prever un amplio proceso de consulta sobre la introducción de las e-TIC que incluya a los actores políticos y de la sociedad civil y tenga en cuenta el más amplio espectro posible de opiniones.
- j) Si se aplica siguiendo las buenas prácticas, el proceso de adopción de las e-TIC puede llevar bastante tiempo, por lo que el OE debe considerar adecuadamente su calendario en relación con el ciclo electoral. Una aplicación precipitada dará lugar

inevitablemente a que algunas partes del proceso no se apliquen plenamente, lo que repercutirá negativamente en la calidad de los resultados y en la confianza que las partes interesadas tendrán en las e-TIC.

- k) El OE y el Parlamento deben garantizar que las e-TIC se introduzcan con la condición de que se disponga del tiempo y la financiación adecuados para su correcta deliberación y aplicación, en consonancia con las buenas prácticas internacionales. Hay que dejar tiempo para que se lleven a cabo los procesos de consulta pública, evaluación de necesidades, estudio de viabilidad, contratación, cambios legislativos, pilotaje, certificación y pruebas, así como para la supervisión parlamentaria y la rendición de cuentas legal. A menudo esto requiere más de un ciclo electoral.
- l) Una tarea fundamental del OE es garantizar la transparencia del proceso en todas sus fases, factor clave para aumentar la confianza de las partes interesadas, lo que incluye tanto dar un acceso significativo a la documentación pertinente a las partes interesadas y a los observadores como mantener informado al público a través de programas de información a los votantes.
- m) El OE tiene la responsabilidad de garantizar que el proceso de implantación de las e-TIC cumple los plazos y los requisitos legales, y de colaborar estrechamente con los proveedores para garantizar el cumplimiento de estos criterios.
- n) El proceso de certificación/auditoría de los sistemas de e-TIC debe ser dirigido por expertos o instituciones independientes, pero los actores nacionales, el OE en primer lugar, deben mantener la responsabilidad general del proceso. Los OE también deben garantizar la transparencia facilitando información sobre las pruebas y la certificación a las que se sometan los sistemas de e-TIC y permitiendo una observación significativa.
- o) Los principios de soberanía exigen que los datos recogidos por el sistema de e-TIC pertenezcan al OE, cumplan las leyes y reglamentos nacionales en materia de transparencia y privacidad y estén sujetos a la jurisdicción de los tribunales nacionales.
- p) Los OE deben garantizar que los datos electorales estén abiertos a todos los ciudadanos para que puedan comprender, evaluar y, en última instancia, aceptar la credibilidad de las elecciones. Los datos recogidos por las e-TIC deben pertenecer al OE, cumplir las leyes y reglamentos nacionales en materia de transparencia y privacidad y estar sujetos a la jurisdicción de los tribunales nacionales.

Otras partes interesadas nacionales:

- q) Las partes interesadas nacionales, los partidos políticos, la sociedad civil (incluidos los observadores electorales) y los medios de comunicación deberían desempeñar un papel importante en los debates inclusivos y amplios sobre la adopción de las e-TIC.
- r) También deberían actuar como guardianes y supervisar el proceso de licitación, prueba, instalación y uso del sistema e-TIC.

Fabricantes y vendedores de e-TIC:

- s) Dada la importancia crítica de las elecciones en la vida democrática de un país, los fabricantes y vendedores de e-TIC deben cumplir requisitos estrictos de responsabilidad y rendición de cuentas corporativa y debida diligencia en materia de derechos humanos, así como requisitos igualmente estrictos de fiabilidad y rendimiento.

Donantes y proveedores de apoyo electoral

- t) Los donantes deberían garantizar que, si apoyan la introducción de tecnología en las elecciones, ésta se base en un análisis independiente e inclusivo para identificar la

tecnología más eficaz para responder a los retos identificados conjuntamente y al contexto socioeconómico dado. Apoyar una evaluación de viabilidad exhaustiva, que incluya evaluaciones de riesgos, costos y sostenibilidad en un proceso inclusivo antes de cualquier decisión de proceder debería ser la práctica habitual.