Propuesta de protocolo

de auditoría para el software de escrutinio de las elecciones de Colombia en 2018

(Artículo 45, Ley 1475 de 2011)

<K+LAB>
SEGURIDAD DIGITAL Y PRIVACIDAD

moe
Misión de Observación Electoral

***Elaborado por**:*
El Laboratorio de Seguridad digital y privacidad de la Fundación Karisma –KLAB
con la colaboración de *La Misión de Observación Electoral –MOE*

Autores:
Pilar Sáenz
Joan López
Santiago Hernández

Con el apoyo de:
Carolina Botero

Diseño y Diagramación:
Paula Camila Cruz Fajardo
Diseñadora Gráfica- Comunicaciones MOE

Bogotá, Colombia
Febrero, 2018.

Tabla de Contenido

Tabla de Contenido

1. Introducción ..... Pág. 5

2. Recomendaciones de los estándares internacionales para auditorías ..... Pág. 9
- 2.1. Acceso a la información y al código fuente ..... Pág. 10
- 2.2. Actualización del marco legal ..... Pág. 11
- 2.3. Trazabilidad ..... Pág. 11
- 2.4. Integridad de la información ..... Pág. 12
- 2.5. Las precauciones de la tercerización ..... Pág. 13
- 2.6. Certificación y auditoría de un organismo independiente ..... Pág. 13

3. Experiencias nacionales ..... Pág. 14
- 3.1. México, la presión por la transparencia ..... Pág. 14
- 3.2. Alemania, una crisis de transparencia ..... Pág. 16
- 3.3. Noruega, cuando la transparencia ayuda a la democracia ..... Pág. 17
- 3.4. Argentina, la crisis de la seguridad por oscuridad Pág.18

4. Propuesta de pruebas para la auditoría Pág.20
- 4.1. Checklist #1. Pruebas básicas de seguridad Pág.21
  - 4.1.1. Pruebas generales Pág.22
  - 4.1.2. Pruebas con usuario administrador Pág.22
  - 4.1.3. Pruebas con usuario no administrador (El utilizado para usar el sistema) Pág.23
- 4.2. Recursos documentales base para la auditoría Pág.24
  - 4.2.1 Software Pág.24
  - 4.2.2. Documentales Pág.24
  - 4.2.3. Certificaciones Pág.24
  - 4.2.4. Resultados de auditorías internas y externas Pág.26
  - 4.2.5. Actas Pág.27
- 4.3. Pruebas de funcionalidad Pág.27
  - 4.3.1. Desarrollo de la prueba Pág.27
  - 4.3.2. Reportes Pág.28
  - 4.3.3. Escrutinio general (Departamental) Pág.28
  - 4.3.4. Consideraciones generales para las pruebas de funcionalidad Pág.28

5. Posibles escenarios para una auditoría al sistema de escrutinio de las elecciones en Colombia Pág.30
- 5.1. Escenario 1. Auditoría documental y pruebas de seguridad básicas Pág.31
  - 5.1.1. Actividades escenario 1 ..... Pág.31
  - 5.1.2. Presupuesto escenario 1 ..... Pág.31
- 5.2. Escenario 2. Auditoría documental, pruebas de seguridad básicas y pruebas de software Pág.32
  - 5.2.1. Actividades escenario 2 ..... Pág.32
  - 5.2.2. Presupuesto escenario 2 ..... Pág.32
- 5.3. Escenario 3. Auditoría documental, pruebas de seguridad básicas, pruebas de software y pruebas de seguridad web Pág.33
  - 5.3.1. Actividades escenario 3 ..... Pág.33
  - 5.3.2. Presupuesto escenario 3 ..... Pág.33

6. Opciones de auditoría para las elecciones de 2018 ..... Pág.35

Bibliografía Pág.39

1 Introducción

Introducción

Desde las elecciones presidenciales de 2014, se han estado celebrando contratos con la Unión Temporal Soluciones Informáticas Electorales (UTSIE) para "prestar el servicio de una solución informática para los procesos de preconteo, escrutinio y digitalización de actas"[1]. La empresa elegida para proveer el servicio es una unión de varias empresas: Carvajal S.A., el Grupo ASD, Data Processing Systems S.A., Manejo Técnico de Información S.A. y Thomas Greg & Sons[2]. Entre los requerimientos se ordenó la utilización de un software de escrutinio y consolidación de los resultados electorales. A pesar de que, por su importancia en para el proceso democrático de un país, internacionalmente hay un consenso sobre la necesidad de garantizar una serie de controles sobre este tipo de software, la Registraduría Nacional del Estado Civil (RNEC) no cuenta con un examen exhaustivo del aplicativo y en los momentos previos a las elecciones se limita a entregar una copia del código fuente que dicen va a ser usado en los comicios a la Procuraduría General de la Nación para su custodia. Igualmente, no se ha actualizado el marco legal del procesamiento de resultados electorales con una explicación clara y detallada del nuevo procedimiento[3].

Existen registros de que la RNEC contrató una auditoría al proceso electoral para las elecciones de congreso, parlamento andino y presidente y vicepresidente prime-

[1] Proceso número 023 de 2013 Registraduría Nacional del Estado Civil (RNEC)

[2] En total se les ha adjudicado 7 contratos entre 2013 y 2017 por una suma de 481 mil millones de pesos. Proceso 023, 053; Contratación Directa 028, 043, 072 y Selección Abreviada 07, 010. Disponibles en: www.contratos.gov.co

[3] Decreto 2241 de 1984

[4] Contrato de prestación de servicios No. 077 de 2014, suscrito entre la Registraduría Nacional de Estado Civil y Unión temporal AUDIDNET 2014. Disponible en https://www.contratos.gov.co/consultas/VerDocumentoPublic?ruta=/cloud/cloud2/2014/C/128001000/14-18-2548458/C_PROCESO_14-18-2548458_128001000_10424428.pdf

ra vuelta, a realizarse en el año 2014[4]. Sin embargo, los resultados de esa auditoría no fueron públicos ni tienen el carácter de una auditoría externa e independiente. De hecho cuando el partido Centro Democrático intentó realizar una auditoría al software de Escrutinio una de las conclusiones que presentaba fue "se desconoce que haya una certificación y soportes de una empresa especializada e independiente, sobre las pruebas y el correcto funcionamiento del mencionado Sistema, más allá de las pruebas y verificaciones realizadas por la Registraduría Nacional en el ejercicio de las interventorías y supervisiones de los contratistas." [5]

Por otra parte, el 8 de febrero de 2018 el Consejo de Estado falló una denuncia del Movimiento Independiente de Renovación Absoluta (MIRA) acerca de un sabotaje en los resultados de las elecciones para el Senado 2014-2018 a través del software de escrutinio alegando manipulación a horas indebidas y accesos no autorizados para modificar los resultados. Para el fallo, el Consejo contactó a peritos informáticos de la Fiscalía que establecieron que fue imposible determinar si hubo sabotaje, pues no contaban con el escenario original tanto del aplicativo como de los dispositivos utilizados en las mesas denunciadas por el MIRA. Para este caso, el código fuente en custodia en la Procuraduría no se usó porque no era posible con esa pieza recrear el escenario y tampoco se podía saber si realmente esa era la versión utilizada. Una muestra de que el software no está hecho para ser controlado se confirma con la afirmación de los propios contratistas durante este proceso. Ellos aseguraron que, por mandato del contrato, eliminaron todos los archivos originales tres meses después de las elecciones.

Sin embargo, con la poca información que se contaba, los peritos encontraron anormalidades como: desactivación del acceso con huella para insertar resultados, archivos sin usuario de soporte, carencia de copias de respaldo y entradas para corregir resultados. Con esto, el Consejo determinó que hubo sabotaje en 3.630 registros de 1.412 mesas y que no se cumplió con la ruta de actividades pactadas por la Registraduría previo a los comicios[6].

Por estas razones, consideramos que la Registraduría está tratando el software como una "caja negra", pues ni el organismo, ni los actores interesados en el proceso electoral conocen de forma exhaustiva el funcionamiento interno del aplicativo. De hecho, enfrentados a los resultados del fallo del 8 de febrero, no se trata de una caja negra como la de los aviones que permite la reconstrucción de lo que sucedió, es una caja negra oscura, cerrada y hermética.
El fallo del Consejo de Estado deja claro que el Organismo Electoral debe tratar al sistema informático de administración electoral con los mismos parámetros legales de cualquier documentación electoral.

Así pues, la situación actual pone en riesgo los derechos de la ciudadanía, pues no conocemos si se cumplen con los requisitos de los estándares internacionales, no contamos con ningún tipo de respaldo para trazar el correcto funcionamiento del sistema electoral y no tenemos mecanismos adecuados de observación electoral de sistemas informáticos[7].

La Registraduría se encuentra obligada desde 2011 por mandato legal a implementar la votación electrónica en el país[8]. Sin embargo, a pesar de la presión del Congreso de la República, la RNEC solamente tiene un marco de requerimientos para proponentes y ha recibido cotizaciones de oferentes[9]. Ahora bien, teniendo en cuenta las experiencias internacionales donde la aplicación del voto electrónico presenta problemas y preguntas abiertas, los retrasos de la Registraduría pueden ser una buena oportunidad para establecer una discusión abierta y constructiva entre

[5] Centro Democrático, Informe de auditoría al sistema informático de escrutinios de la Registraduría nacional de estado civil. Marzo 2014. Disponible en http://www.centrodemocratico.com/sites/default/files/wp-content/uploads/2014/03/Informe-Auditor%C3%ADa-Nacional-de-Sistemas-CD.pdf
[6] Colombia. Consejo de Estado. Sala de lo Contencioso Administrativo. Sección quinta. Fallo Electoral del 8 de febrero de 2018.
[7] La RNEC se limita a permitir la observación del momento en el que se ingresan los datos al software.
[8] Registraduría Nacional del Estado Civil, Ley 1475 de 2011. Capítulo 4. Disponible en https://www.registraduria.gov.co/IMG/pdf/ley_1475_2011.pdf

los actores interesados. En este momento, la Registraduría ha incorporado ampliamente sistemas electrónicos que deben ser discutidos con la misma seriedad y transparencia con la que sería abordado cualquier cambio en el sistema electoral.

Los Sistemas de Administración Electoral se pueden clasificar en manuales, híbridos y electrónicos. Entre los sistemas híbridos están: el registro electrónico de votantes, la transmisión de resultados por medios magnéticos o digitales y la utilización de aplicativos para consolidar y publicar los resultados. A su vez, los electrónicos se dividen en: conteo electrónico por medio de software de reconocimiento como OCR (Optical Character Recognition) o OMR (Optical Mark Recognition), votación electrónica en máquinas de grabación directa (DRE por sus siglas en inglés) y la votación por internet[10].

Con fundamento en lo anterior, podemos decir que el sistema colombiano está en la categoría híbrida. Colombia ha incorporado sistemas electrónicos y, sin embargo, una mirada a los estándares internacionales para este tipo de ejercicios nos permite concluir que el país no está cumpliendo con los requisitos de transparencia y, sobre todo no sabemos si cumple con los requerimientos técnicos. Aunque parece estar contemplada como una parte del proceso de desarrollo del software de elecciones, en realidad hace falta una auditoría del proceso electoral profesional e independiente de la Registraduría, con resultados públicos y que de garantías sobre el sistema. Más allá de este hecho, la Registraduría tampoco ha facilitado el ejercicio de auditorías y controles independientes como los que se promueven en la ley 1475 de 2011, donde se estipula que "los partidos, movimientos y grupos significativos de ciudadanos, que inscriban candidatos a cargos o corporaciones de elección popular o promuevan el voto en blanco, así como las organizaciones de observación electoral reconocidas por el Consejo Nacional Electoral, tienen derecho a ejercer vigilancia de los correspondientes procesos de votación y escrutinios, para lo cual podrán acreditar ante el Consejo Nacional Electoral los testigos electorales por cada mesa de votación y por cada uno de los órganos escrutadores. Cuando se trate de procesos a los que se han incorporado recursos tecnológicos, se podrán acreditar también auditores de sistemas."[11] De nuevo, la forma como la Registraduría aborda la incorporación de sistemas electrónicos es como si fuera "una caja negra" y eso, como veremos, no es una mirada acorde con las prácticas internacionales. Si este es el camino que plantea el organismo electoral, se generan serias preocupaciones sobre el procedimiento que se está llevando a cabo de implementación del sistema de administración electoral con apoyo electrónico. Asimismo, la denuncia del MIRA muestra que el camino que sigue el Organismo Electoral genera serias preocupaciones sobre el sistema de administración electoral con apoyo electrónico.

Efectivamente, uno de los principios que todo gobierno debe seguir para la adopción de sistemas electrónicos en procesos electorales es la transparencia que consigue superar la idea de que el sistema es una "caja negra" insondable y por el contrario, mediante verdaderos y efectivos instrumentos, entre ellos las auditorías, es posible analizar lo que sucede durante el proceso electoral y buscar la tranquilidad de que no ha sido indebidamente manipulado. Aunque en Colombia existe la obligación legal de permitir la auditoría (artículo 45 de la Ley Estatutaria 1475 de 2011) hasta la fecha los ejercicios que se han hecho no tienen las características técnicas de una auditoría y tampoco se han establecido los parámetros con que esta auditoría debería hacerse.

El Consejo de Estado determinó que la Organización Electoral debería cumplir tres requisitos para las siguientes elecciones que ratifican los estándares

[9] RNEC. Acta 30 del 10 de marzo de 2016. (RNEC,2016); RNEC. Informe de gestión 2016. (RNEC, 2016)
[10] United Nations Development Program (UNDP). Electoral Results Management Systems: Catalogue of Options A guide to support electoral administrators and practitioners to evaluate RMS options, benefits and challenges. (UNDP, 2015), 43-45.
[11] Idib. Ley 1475 de 2011 Art. 45.

internacionales. Primero, adquirir el software de escrutinio "desde y para el Estado", con completa trazabilidad de actividades y con personal idóneo dentro del Estado para el soporte técnico especializado. Segundo, implementar medidas para mantener los ordenadores actualizados y con copias de seguridad. Tercero, resguardar "los archivos Log tanto del sistema operativo de los equipos donde funcione el software de escrutinio, como los de la base de datos y los del software mismo"[12].

El presente documento tiene como finalidad principal proponer una herramienta que permita la efectiva concreción de esa obligación legal y la construcción de confianza entre las partes interesadas por medio de una transparencia efectiva. Es decir, ofrecer un protocolo para auditorías de sistemas electrónicos que pueda implementarse al proceso electoral colombiano en 2018 en el marco del artículo 45 de la Ley Estatutaria 1475 de 2011 que permita a los partidos políticos y a la Misión de Observación Electoral (MOE) hacer uso de esa facultad legal.

Con este propósito el presente documento revisa cuales son las recomendaciones derivadas de estándares internacionales en auditorías y transparencia de sistemas electrónicos en elecciones, analiza otras experiencias que pueden servir de referencia, presenta una propuesta de pruebas para la realización de auditorías de diferente profundidad para el software de escrutinio, plantea posibles escenarios para la realización de auditorías y finalmente introduce una propuesta de auditoría de revisión intermedia que podría implementarse para el ejercicio electoral de 2018 en Colombia.

[12]CE. Fallo electoral del 8 de febrero de 2018.

2 Recomendaciones de los estándares internacionales para auditorías

Recomendaciones de los estándares internacionales para auditorías

Los estándares de inclusión de Tecnologías de la Información y las Comunicaciones (TIC) en procesos electorales que se utilizaron para este análisis provienen de variadas fuentes, puesto que, como se mostró anteriormente, el tema es complejo y cuenta con muchas aristas sociales y tecnológicas.

En primer lugar, se analizaron estándares construidos por organizaciones intergubernamentales como el Consejo Europeo[13], la Organización para la Seguridad y la Cooperación en Europa (OSCE)[14] y el Programa de las Naciones Unidas para el Desarrollo (UNDP)[15]. En segundo lugar, en Estados Unidos cada Condado tiene la libertad de elegir el sistema que va utilizar y esto ha significado la proliferación en ese país de una gran variedad de sistemas. En un intento por estandarizar toda esta multiplicidad y asegurarse que los sistemas cumplan con unos requisitos mínimos aparecieron guías creadas por la Comisión de Asistencia Electoral (EAC)[16]. En tercer lugar, están los actores regionales que tratan de guiar la aplicación de TICs en las elecciones: el Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) en Argentina[17], la Misión de Observación Electoral (MOE) en Colombia[18] y la Organización de Estados Americanos (OEA)[19]. Finalmente, se analizaron los estándares construidos por organizaciones sin ánimo de lucro a nivel internacional para incentivar sistemas que sean más participativos, transparentes y seguros. Entre estas organizaciones están: el Instituto Internacional para la Democracia y Asistencia Electoral (IDEA)[20], la Fundación Internacional para los Sistemas Electorales (IFES)[21] y el Centro Carter[22].

[13] Council of Europe. Certification of e-voting systems Guidelines for developing processes that confirm compliance with prescribed requirements and standards. (Strasbourg: CoE, 2011)
Council of Europe. LEGAL, OPERATIONAL AND TECHNICAL STANDARDS FOR E-VOTING. (Strasbourg: CoE, 2004)
[14] OSCE Office for Democratic Institutions and Human Rights. Handbook For the Observation of New Voting Technologies. (Warsaw: OSCE, 2013)
OSCE Office for Democratic Institutions and Human Rights. Election Observation Handbook. (Warsaw: OSCE, 2010)
[15] UNDP, Electoral Results Management Systems
[16] Election Assistance Commission. Voting System Testing and Certification Program. (Washington: EAC, 2011)
Election Assistance Commission. Voluntary Voting System Guidelines. (Washington: EAC, 2005)
[17] CONICET, Análisis De Factibilidad En La Implementación De Tecnología En Diferentes Aspectos Y Etapas Del Proceso Electoral (Buenos Aires: CONICET, 2017).
[18] Misión de Observación Electoral, Implementación Del Voto Electrónico En Colombia (Bogotá: MOE, 2014).
[19] Organización de los Estados Americanos, Tecnologías Aplicadas Al Ciclo Electoral (OEA, 2014).
[20] International Institute for Democracy and Electoral Assistance. Introducing Electronic Voting: Essential Considerations. (Stockholm: IDEA, 2011)
International Institute for Democracy and Electoral Assistance. Certification of ICTs in Elections. (Stockholm: IDEA, 2015)
International Institute for Democracy and Electoral Assistance. International Electoral Standards Guidelines for reviewing the legal framework of elections. (Stockholm: IDEA, 2002)
[21] International Federation for Electoral Systems. Electronic Voting & Counting Technologies A Guide to Conducting Feasibility Studies. Edited by Ben Goldsmith. (Washington: IFES, 2011)
National Democratic Institute for International Affairs (NDI), and International Foundation for Electoral Systems (IFES). Implementing and Overseeing Electronic Voting and Counting Technologies. (Washington: IFES & NDI, 2013)
[22] The Carter Center. Developing a Methodology for Observing Electronic Voting. (Atlanta: The Carter Center, 2007)
The Carter Center. The Carter Center Handbook on Observing Electronic Voting. (Atlanta: The Carter Center, 2012)

A continuación se identificarán algunos de las recomendaciones en común que tienen los estándares anteriormente enunciados en búsqueda de sugerir el mejoramiento del sistema electoral y construir confianza en todas las partes interesadas.

2.1 *Acceso a la información y al código fuente*

Algo que comparten los estándares analizados es la necesidad de que los sistemas respondan a un principio de transparencia para con todos los actores interesados. Todos los ejercicios de transparencia tienen como objetivo garantizar los derechos de la ciudadanía tanto en la parte manual del proceso como en la digital para generar confianza en el sistema electoral[23].

Se trata de un requerimiento que debe ir más allá de la mera observación del proceso de transmisión de información que desde 2014 ha implementado la Registraduría como ejercicio de transparencia y que, a todas luces resulta en una actividad insuficiente y que no puede ser considerada como desarrollo de la obligación legal del artículo 45. En otras palabras, no se debe igualar el proceso de observación electoral de sistemas manuales con los electrónicos[24].

Los documentos analizados generan tres recomendaciones en términos de transparencia para la Registraduría:

- En primer lugar, todos los actores deben tener acceso a la documentación completa de cotización, compra y funcionamiento interno del software electoral[25].Esto incluye toda la documentación generada durante el desarrollo del software como diseño, arquitectura y especificaciones[26].
- En segundo lugar, los actores como los partidos, entes de control y de observación electoral deberían tener una copia del código fuente para auditoría. Se debe asegurar que el código entregado sea el mismo utilizado durante el proceso electoral. Por este motivo debe haber un cierre sobre el desarrollo del mismo al menos dos meses antes de las elecciones. Igualmente, los entes internacionales recomiendan la contratación de personal experto entre los actores para el análisis del software[27]. Asimismo, la entrega del software se debe hacer con suficiente tiempo para garantizar un análisis exhaustivo previo a las elecciones[28].
- Por último, se recomienda tener protocolos de observación electoral tanto para las actividades manuales como para las electrónicas[29]. Precisamente, se trata de clarificar que no es lo mismo un sistema de votación híbrido que uno manual y por tanto deben tener sistemas de monitoreo diferenciados.

El artículo 45 provee el marco legal para desarrollar esta recomendación, sin embargo, su implementación está lejos de ser adecuada.

[23] The Carter Center. The Carter Center Handbook, 26.
[24] UNDP, Electoral Results Management Systems, 11.
[25] NDI & IFES. Implementing and Overseeing Electronic Voting, 41-43; IDEA. Certification of ICTs; The Carter Center. The Carter Center Handbook, 34; CoE. Certification of e-voting systems, 5; OSCE ODIHR. Handbook For the Observation, 11; UNDP. Electoral Results Management Systems, 87.
[26] CONICET. Análisis de factibilidad, 12.
[27] NDI & IFES. Implementing and Overseeing Electronic Voting, 44; IDEA. Introducing Electronic Voting, 13; IDEA. Certification of ICTs, 46; CoE. LEGAL, OPERATIONAL AND TECHNICAL, 11; OSCE ODIHR. Handbook For the Observation, 26; UNDP. Electoral Results Management Systems, 76, The Carter Center. Developing a Methodology, 4-6.
[28] CONICET, Análisis de factibilidad, 12.
[29] OSCE ODIHR. Handbook For the Observation, 11.

2.2 Actualización del marco legal

Los estándares internacionales reclaman que se tenga un marco legal coherente con las ventajas y peligros que encarna la aplicación de TIC en los sistemas electorales. Por esta razón, al implantar una nueva tecnología se debe actualizar la legislación para dejar establecido de manera clara y detallada el proceso de escrutinio y consolidación electoral, incluyendo los nuevos dispositivos y aplicativos que se utilizan[30].

En cuanto a esto, Colombia tiene una importante deuda, pues el sistema de administración electoral funciona sin un marco legal actualizado para los nuevos procedimientos y tecnologías introducidas en el sistema[31]. Igualmente, las organizaciones preocupadas por las tecnologías electorales señalan repetidamente la necesidad de que el marco legal establezca procedimientos de auditoría y obligue a la Registraduría a efectuar estas pruebas de forma recurrente[32]. En esto la norma colombiana incluye la obligación, pero no la ha implementado debidamente.

2.3 Trazabilidad

Otro factor importante para garantizar unas elecciones seguras es la capacidad de trazar las modificaciones que se le hagan tanto al software de tabulación como a los datos ingresados parcialmente. Las organizaciones internacionales recomiendan cuatro prácticas para evitar fraudes electorales a través de las herramientas tecnológicas aplicadas en los sufragios:

1. Sobre el proceso de desarrollo

Los estándares resaltan que en el proceso de desarrollo no debería haber cambios al sistema a menos que sean aceptados por los actores, se haga la correspondiente auditoría y se actualice el sistema en todos los dispositivos.

Cada vez que se arreglen errores, el fabricante debe ofrecer pruebas de corrección del sistema[33].

Se deben establecer minutas de ingreso al software por parte tanto de los funcionarios como de los vendedores.

Finalmente, el informe del aplicativo debe ser capaz de identificar quién ingresó, cuándo lo hizo y qué ingresó al sistema[34].

2. Identificación en el sistema

Las entidades internacionales establecen que se debe generar identificación diferenciada para el funcionario que ingresa los datos y para la máquina utilizada[35]. De esta forma, se hace posible cotejar que la información agregada provenga de fuentes autorizadas.

3. Auditorías

Asimismo, una recomendación protocolaria es una auditoría previa y una posterior a los comicios para asegurarnos que se está utilizando el mismo software y no recibió ningún tipo de modificación no autorizada[36].

4. Double blind entry

De la misma manera, se recomienda utilizar el Double blind entry que sugiere cambiar la forma en que se ingresan los datos en el sistema. En este tipo de metodología se requiere que dos funcionarios digiten

[30] IDEA. Certification of ICTs; IDEA. International Electoral Standards, 79; The Carter Center. Developing a Methodology, 6; CoE. LEGAL, OPERATIONAL AND TECHNICAL, 11; EAC. Voluntary Voting System Guidelines.
[31] Como s e mencionó anteriormente, el marco legal electoral es de 1984
[32] NDI & IFES. Implementing and Overseeing Electronic Voting, 194; IDEA. Certification of ICTs, 20.
[33] ISO 15488
[34] OSCE ODIHR. Handbook For the Observation, 26- 33; EAC. Voluntary Voting System Guidelines; UNDP. Electoral Results Management Systems, 76.
[35] EAC. Voluntary Voting System Guidelines; UNDP. Electoral Results Management Systems, 85
[36] IDEA. Introducing Electronic Voting 24.

los resultados al sistema de forma paralela, pero separados físicamente, con equipos diferentes y sin conocimiento de quién es el segundo encargado[37]. Así, podemos cotejar la información ingresada y determinar si ha habido un intento de fraude.

Además, en búsqueda de asegurar la trazabilidad y generar evidencias legales y técnicamente viables para procesos de investigación posteriores, los sistemas informáticos deben generar logs de auditoría en todas sus transacciones y sobre todos los elementos que los conforman (Sistemas operativos, bases de datos, elementos de seguridad, etc.). Estos logs deben ser almacenados de forma segura en un lugar centralizado que permita demostrar que no han sido alterados (Forensically sound[38]). De hecho Dentro del peritaje del software realizado por la Fiscalía se descubrió que el sistema utilizado no genera logs en una gran parte de sus módulos o de los sistemas auxiliares que lo conforman. Igualmente, se demostró que asegurar la trazabilidad del sistema actual es imposible ya que no se producen valores hash sobre las versiones del software o de los logs generados por el mismo. Estos valores hash son la única forma técnica con validez legal de poder demostrar que no hubo cambios sobre el mismo después de que fueron generados[39].

2.4 *Integridad de la información*

Todas estas recomendaciones tienen que estar enmarcadas en procedimientos apropiados para mantener la integridad de la información en casos de emergencia o posibles intentos de fraude. Igualmente, en este punto se pueden identificar 4 buenas prácticas internacionalmente:

- En primer lugar, se hace necesario hacer una copia de replicación[40] debidamente resguardada por un tercero imparcial con toda la información ingresada en el sistema para que, en caso de emergencia, podamos recuperar integralmente los datos que se han ingresado[41]. El fallo del Consejo de Estado demostró que es insuficiente el ejercicio de la Registraduría de entregar la copia del código fuente a la Procuraduría dado que no cumple con los requisitos técnicos para hacer que esta medida sea efectiva. Al ser imposible garantizar reconstruir el estado del sistema, se trata de un ejercicio protocolario que no cumple el propósito para el que existe y, por tanto, no puede considerarse como ajustado al estándar internacional.
- En segundo lugar, las organizaciones internacionales sugieren la creación de un Trigger o un software capaz de identificar inconsistencias en los datos ingresados a través de los mecanismos que mencionamos anteriormente para mantener datos para cotejar[42].
- En tercer lugar, se debe analizar el flujo de la información para encontrar vulnerabilidades en los puntos en que se mueve los datos de un punto a otro[43]. Esto resulta imposible sin la información apropiada sobre los procedimientos y los protocolos establecidos por el marco legal.

[37] Electoral Results Management Systems, 76.
[38] McKemmish R. (2008) When is Digital Evidence Forensically Sound?. In: Ray I., Shenoi S. (eds) Advances in Digital Forensics IV. DigitalForensics 2008. IFIP — The International Federation for Information Processing, vol 285. Springer, Boston, MA
[39] El fallo del Consejo de Estado estableció que "No existían valores hash1 o parámetros que permitieran demostrar técnicamente que las aplicaciones y versiones mostradas por la RNEC y el contratista en las inspecciones judiciales correspondían a las mismas utilizadas para dicho escrutinio"; ii) "No se logró ubicar un equipo de cómputo utilizado en dicho proceso"; iii) "No se conservaron log de eventos de sistema operativo, ni log de bases de datos de los sistemas de información para realizar un análisis técnico con relación a posibles accesos no autorizados a los equipos o a las bases de datos, sino que solo se cuentan con los log de aplicación, los cuales registran las actividades de las comisiones escrutadoras con posterioridad al ingreso al sistema. Estos archivos incluyen modificaciones a los datos que hayan sido avaladas a través de huella dactilar o clave" y iv) "Los archivos log de aplicación tampoco cuentan con un valor hash o huella digital que garantice su integridad e inmodificabilidad, que demuestre técnicamente que se trata de los mismos generados por los aplicativos utilizados en el momento de los tales escrutinios de Senado 2014"
[40] La copia de replicación consiste en mantener una copia de los datos en diferentes sitios. La copia réplica puede ser marcada como de solo lectura y no permite que se modifique para garantizar la integridad de la información.
[41] EAC. Voluntary Voting System Guidelines; UNDP. Electoral Results Management Systems,76.
[42] EAC. Voluntary Voting System Guidelines; UNDP. Electoral Results Management Systems, 77.
[43] The Carter Center. Developing a Methodology, 4; Electoral Results Management Systems, 78.
[44] UNDP. Electoral Results Management Systems, 78.

- Finalmente, después de clarificar los puntos de contingencia y vulnerabilidades se deberían especificar protocolos seguros para mover la información por medios magnéticos que aseguren la confiabilidad e integralidad de la información electoral[44].

2.5 Las precauciones de la tercerización

Muchos gobiernos se han decidido por subcontratar con algún privado las tecnología que utilizan en las elecciones. Sin embargo, gracias a los descuidados contratos existe un riesgo latente para la transparencia y la seguridad de estos sistemas. Teniendo en cuenta que la democracia exige la apertura de la información electoral, los vendedores no deberían poder esconder el funcionamiento de un software electoral aduciendo derechos de autor[45]. Sin embargo, la realidad es que muchos privados encargados del software esconden su código fuente y su documentación del escrutinio de los actores electorales y la ciudadanía detrás de la titularidad que pueden ostentar sobre el software que están contratando, esta práctica va en contravía con los deberes democráticos[46].

En el caso que se contrate el desarrollo del software, se debe aclarar contractualmente que toda la información del software debe estar disponible públicamente[47]. Asimismo, la contratación requiere de experticia dentro del organismo de administración electoral, pues, de lo contrario, se está perdiendo el carácter público y transparente de las elecciones, al generar dependencia total de los privados[48]. Además, el software debe contar con una certificación de calidad y seguridad internacional y explicitar cómo cumple los estándares internacionales para sistemas electorales[49].

Para cumplir a cabalidad con la transparencia que debería caracterizar a estos programas, varios de los organismos internacionales recomiendan el uso de software de código abierto. Consideran que es el sistema más compatible con las características requeridas en las elecciones. Este tipo de sistemas son transparentes (están disponibles para la ciudadanía), seguros (son auditados y mejorados constantemente por expertos) y mucho más económicos que el software privativo (argumento esencial en la inclusión de TICs en elecciones)[50].

2.6 Certificación y auditoría de un organismo independiente

Una recomendación muy importante que comparten todos los organismos internacionales es la necesidad de una certificación de calidad y seguridad de un organismo independiente a los partidos políticos, la Registraduría y al vendedor de software[51]. Asimismo, los resultados de la auditoría deben ser de carácter público y accesible para cualquier ciudadano con interés de comprobar la confiabilidad del sistema[52].

[44]UNDP. Electoral Results Management Systems, 78.
[45]NDI & IFES. Implementing and Overseeing Electronic Voting, 175; IDEA. Introducing Electronic Voting, McGaley, Margaret, and Joe McCarthy. "Transparency and E-Voting: Democratic Vs. Commercial Interests." Electronic Voting in Europe 47 (2004): 153-63.
[46]Massey, Andrew. "But We Have to Protect Our Source: How Electronic Voting Companies' Proprietary Code Ruins Elections." Hastings Comm. & Ent. LJ 27 (2004): 233.
[47]UNDP. Electoral Results Management Systems, 87; IDEA. Introducing Electronic Voting, 13
[48]NDI & IFES. Implementing and Overseeing Electronic Voting, 43; IDEA. Certification of ICTs, 13
[49]UNDP. Electoral Results Management Systems, 105.
[50]NDI & IFES. Implementing and Overseeing Electronic Voting, 42; El Programa de las Naciones Unidas para el Desarrollo ha esta ayudando a varios gobiernos a implementar software de código abierto para elecciones como el caso de Libia. En: UNDP. Electoral Results Management Systems, 86.
[51]NDI & IFES. Implementing and Overseeing Electronic Voting, 44; IDEA. Certification of ICTs, 48; IDEA. International Electoral Standards, 78; The Carter Center. Developing a Methodology, 7; UNDP. Electoral Results Management Systems, 87.
[52]CONICET, Análisis de la factibilidad, 12.

Estos son los puntos comunes que hemos identificado como alertas o recomendaciones entre las entidades que se han preocupado por la utilización de TICs en el sistema electoral de un país. La falta de transparencia que ha habido en el proceso colombiano ha dificultado que se pueda cotejar el cumplimiento de los estándares internacionales y, en el caso de no cumplirse, las razones que sustentan su carencia. Esta afirmación se hace a pesar de que, aunque Colombia no ha hecho una actualización normativa para recoger los retos y beneficios que suponen la incorporación de TIC en el proceso electoral, sí se debe resaltar que en el artículo 45 de la Ley Estatutaria 1475 de 2011 se establece que los partidos políticos y la Misión de Observación Electoral están facultados para hacer una auditoría del software. Sin embargo, esta posibilidad no se ha desarrollado en la realidad.

A continuación, se explorarán algunos casos nacionales que sustentan las dificultades a las que se puede enfrentar una autoridad electoral al momento de implementar tecnologías en el sistema de administración electoral. Esto con el interés de aprender de los errores de otros sistemas y las oportunidades que presentan para construir un camino apropiado para modernizar el sistema colombiano con transparencia y construyendo la confianza de todas las partes interesadas.

3 Experiencias nacionales

Experiencias nacionales

3.1 México, la presión por la transparencia

Las auditorías de la aplicación de TICs en sistemas electorales no se limitan a sistemas totalmente electrónicos, sino también a sistemas híbridos. En México, para las elecciones federales de 1991 el Instituto Nacional Electoral (INE) comenzó a utilizar el Sistema de Resultados Electorales Preliminares (SIRE) para proporcionar información inmediata. Sin embargo, lejos de ser un sistema complejo se trataba de un centro de recepción de resultados en fax que luego eran comunicados a la prensa por vía telefónica[53]. A partir de esta experiencia, para las elecciones de 1994 apareció el Programa de Resultados Electorales Preliminares (PREP) el primer sistema electrónico para el procesamiento de resultados electorales. Para 1997, con una auditoría hecha por el INE del SIRE y el PREP anterior, se realizó una reestructuración para que la transmisión de los resultados fuera inmediata y por diferentes medios (magnéticos, telefónicos y fax)[54].

[53] Instituto Federal Electoral (IFE). PREP 2000. Conteo rápido. (INE, 2002), 17.
[54] Ibid., 19

Para las elecciones del año 2000, el INE hizo los primeros esfuerzos de transparencia que incluían la publicación de notas de prensa detalladas y una presentación pública frente a la Universidad Iberoamericana, el PNUD y la Embajada de los Estados Unidos. Asimismo, en 2002 se inició la publicación de memorias que daban cuenta de fundamentos legales, algunas características operativas y los mecanismos de seguridad con los que contaba el PREP[55]. Para las Elecciones de 2006, la carencia de transparencia y el interés de sostener una buena imagen internacional y no nacional, generó que, ante unos resultados muy reñidos, la opinión pública hablara de un fraude electoral a través del PREP[56]. Con la presión de la opinión pública, en 2009 se hizo un convenio entre el Instituto Federal Electoral (IFE) y la Universidad Autónoma de México (UNAM) para realizar una serie de recomendaciones sobre el PREP[57].

El INE dio un paso adelante en transparencia para las elecciones de 2012, firmando un convenio con la UNAM para hacer una auditoría técnica del sistema PREP por medio de pruebas funcionales de caja negra y una revisión visual del código fuente[58]. Asimismo, el convenio establecía la publicación de los resultados de la auditoría en la página del INE y la construcción de un protocolo de auditoría para ser presentado frente a los actores interesados en los resultados electorales[59]. A partir de estas elecciones, las auditorías del PREP se convirtieron en una buena práctica para las elecciones federales y para los siguientes comicios de julio del 2018 ya se ha iniciado la labor[60]. Igualmente, el PREP actualmente se utiliza en las elecciones de los Estados de Colima, Ciudad de México, Sinaloa y Aguascalientes, y cada Estado realiza una auditoría autónoma por comunidades expertas y los resultados se publican en la página del INE. En general, los resultados de las auditorías han sido satisfactorios, pero siempre se hacen recomendaciones que se incluyen en la siguiente versión del software. De la misma forma, la participación de la comunidad experta y la transparencia con la ciudadanía han generado un ambiente de confianza en el software, a pesar de la crisis institucional que vive actualmente el gobierno mexicano.

El caso de México muestra la importancia de las auditorías realizadas por terceros para construir confianza entre todas las partes interesadas en el sistema electoral. Igualmente, resulta interesante el esfuerzo de transparencia de la administración electoral mexicana teniendo en cuenta que el software es para procesar los resultados preliminares. Por el contrario, en Colombia existe un software para el preconteo y otro para escrutinio de los resultados definitivos y ninguno de los dos cuentan con una auditoría externa. Otro esfuerzo de sistemas híbridos que deberían ser ejemplares para Colombia es el uso de software de código abierto como es el caso de Libia que ha construido su aplicativo con el apoyo del Programa de las Naciones Unidas para el Desarrollo[61].

[55]Ibíd. 21
[56]Javier Aparicio, "Análisis Estadístico De La Elección Presidencial De 2006 ¿Fraude O Errores Aleatorios?", PolíticaY Gobierno, 2009, 225-243.
[57]CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12
[58]Instituto Federal Electoral (IFE) & Universidad Autónoma de México (UNAM). "Informe de la aplicación de recomendaciones de la revisión de código fuente y de las pruebas funcionales de caja negra del PREP 2012". (INE, 2012).
[59]Organización de los Estados Americanos (OEA). "Informe final de la misión de observación electoral de la organización de los estados americanos sobre el proceso electoral federal 2011-2012". (OEA, 2012), 18.
[60]Crónica, "La UNAM Auditará El Programa De Resultados Electorales Preliminares Que Se Usará En Julio", 2018, http://www.cronica.com.mx/notas/2018/1059207.html.
[61]UNDP, Electoral Results Management, 43.

3.2 *Alemania, una crisis de transparencia*

Desde 1999, el Estado alemán expidió regulaciones estableciendo el tipo de máquinas y software que podían ser utilizado en las elecciones regionales. Dichas máquinas y software fueron evaluadas por el Departamento Nacional de Metrología y fue certificado por el Ministerio del Interior[62]. En 2005, la ciudad de Hamburg y el Estado de Bayern comenzaron a plantear la posibilidad de usar las mismas máquinas DRE que eran usadas en Holanda construidas por la empresa NEDAP. Igualmente, en ese mismo año se usaron las máquinas NEDAP en cerca de 2000 distritos para las elecciones federales.

En 2006, los activistas del Chaos Computer Club (CCC) comenzaron a escribir reportes resaltando los peligros que podía tener este tipo de máquinas. Dichos reportes se levantaron gracias a la cooperación de los activistas holandeses "Wij vertrouwen stemcomputers niet" quienes compraron una máquina de NEDAP y lograron hackearla[63]. Así en octubre de 2006, un grupo de ciudadanos levantó una petición al Bundestag para prohibir el uso de estas máquinas por sus fallas de seguridad y su falta de transparencia. Sin embargo, el Bundestag dejó claro que esas preocupaciones no eran suficientes para eliminar un sistema que resultaba muy rápido y efectivo. Por esto, los activistas decidieron levantar una demanda contra el sistema ante la Corte Constitucional Federal. Con esto, en 2009, la Corte declaró que se prohibía el uso de este tipo de máquinas para las elecciones federales por problemas de transparencia con la ciudadanía. En otras palabras, hasta que no se pudiera asegurar que cualquier ciudadano pueda entender observar y auditar este tipo de tecnologías, no podían utilizarse en un proceso democrático[64].

El mandato de la Corte Constitucional solo impidió el uso de votación electrónica para tomar los votos, pero se siguieron utilizando tecnologías en los pasos de registro y consolidación de los resultados electorales. El software utilizado para estas operaciones en la mayoría de los Estados es PC-Wahl creado por el grupo Vote ID. Este software es usado en muchas de las elecciones regionales, distritales, federales, europeas y referéndums en Alemania[65]. De la misma forma que con la votación electrónica, otro de los softwares utilizados en Alemania es Votemanager4 que, a su vez, era usado en Holanda hasta que se le encontraron graves fallos de seguridad a principios de 2017[66]. Para este año, ante la presión pública, el Congreso está discutiendo la utilización de este tipo de softwares en el proceso de administración de los resultados electorales[67].

Ante el caso holandés y varias preocupaciones mostradas por los partidos y el público general en 2016, los activistas del CCC decidieron hacer una auditoría del sistema PC-Wahl en su versión 10 que fue utilizado en las elecciones nacionales de 2017[68]. Desde 2016, varias organizaciones han pedido acceso al código fuente del sistema a través de mecanismos legales, pero se les ha negado aduciendo la importancia de ocultar el código para la seguridad del mismo[69]. Por esta razón, sin el código fuente, CCC construyó escenarios para atacar el sistema y encontró graves vulnerabilidades que permitirían al atacante cambiar los resultados de las elecciones. Los problemas encontrados son los siguientes: las protecciones insuficientes para los servidores utilizados en la distribución y operación del

[62] Volkamer, Melanie. "Electronic Voting in Germany." In Data Protection in a Profiled World, 177-89: Springer, (2010)
[63] Jacobs, Bart., & Pieters, Wolter. (2009). Electronic Voting in the Netherlands: from early Adoption to early Abolishment Foundations of security analysis and design V (pp. 121-144): Springer.
[64] Bundesverfassungsgericht, Use Of Voting Computers In 2005 Bundestag Election Unconstitutional (Berlin, 2009).
[65] Thorsten Schröder et al., Analyse Einer Wahlsoftware (CCC, 2017).
[66] Ibíd. 3.
[67] Nederlandse Grondwet. Evaluatie Van De Tweede Kamerverkiezing, 2017. Disponible en: https://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vkf8vkdibryu
[68] The Guardian, "German Hackers Find Security Hole In Software Used For Vote Counts", 2017, https://www.theguardian.com/world/2017/sep/08/german-hackers-find-security-hole-in-software-used-for-vote-counts.
[69] Schröder et al., Analyse Einer Wahlsoftware, 4.

software, la ausencia de cifrado y firmas de seguridad en los resultados transmitidos, el inadecuado cifrado en la información de acceso para la transmisión de resultados y la falta de revisión de autenticidad para el software mismo y sus actualizaciones[70]. A pesar de los esfuerzos de CCC y el caos en Holanda, el organismo de administración electoral decidió utilizar el software[71]. Inclusive, a pesar del mandato de la Corte Constitucional, Estados como Bayern o Rheinland-Pfalz siguen utilizando sistemas de conteo electrónico que se suponen prohibidos en las elecciones alemanas[72].

El caso alemán muestra la importancia de la transparencia en construir confianza en el sistema electoral. En dos oportunidades la falta de transparencia ha llevado a aplicar sistemas con grandes carencias en términos de seguridad digital. A pesar de que la implementación descuidada y apresurada del voto electrónico mostró que las tecnologías en el ciclo electoral podían poner en riesgo el adecuado desarrollo de las elecciones, países como Holanda y Alemania siguen utilizando programas antiguos, oscuros e inseguros. Resulta importante que Colombia aprenda de los casos internacionales para utilizar tecnologías a la altura de las necesidades de la democracia en el siglo XXI, con los estándares de seguridad necesarios para las oportunidades y riesgos las TIC.

3.3 *Noruega, cuando la transparencia ayuda a la democracia*

En Noruega el caso no es de software de escrutinio y consolidación, pero es un buen ejemplo de la importancia de la transparencia con todos los actores interesados para asegurar la protección de los derechos de la ciudadanía. Entre 2004 y 2006, el gobierno noruego comisionó un estudio de factibilidad para implementar el voto electrónico, pero en el informe se determinó que una buena posibilidad sería hacer uso de la votación por internet[73]. Esto con el objetivo de aumentar el índice de participación entre la población joven y la que habita en zonas de climas difíciles Así, en 2008 se creó la organización encargada "E-valg 2011" para determinar los requerimientos, los casos de uso y realizar los respectivos concursos para seleccionar al proveedor del sistema. En 2009 se seleccionaron dos vendedores para preparar el software de las elecciones 2011 y con el objetivo de masificar el uso para 2017[74].

Con algunos retrasos y mucha crítica de la academia y la oposición, se puso en marcha el piloto de votación por internet en diez distritos donde un 26% de los votantes posibles utilizaron el sistema. Para 2012, con un estrecho margen, el congreso decide continuar el piloto para 2013 con un proveedor de software y algunas mejoras en términos de anonimización del voto. En 2013, se aumenta a doce el número de distritos y la cantidad de votantes que utilizaba el sistema aumentó a un 33%. El piloto de 2013 contó con todos los estándares necesarios:

mecanismos de retroalimentación, sistemas de monitoreo, el código fuente se hizo público (a pesar de estar protegido por licencia de software privativo), el organismo de administración electoral organizó una auditoría, se contrató la auditoría de un tercero para el aplicativo y se invitó a organizaciones internacionales como el Centro Carter a auditar el sistema[75].

[70]bíd.,23-24.
[71]The Guardian, "German Hackers Find Security Hole".
[72]Schröder et al., Analyse Einer Wahlsoftware, 23.
[73]Kommunal og Regional Departementet, Electronic Voting: Challenges And Opportunities (Oslo, 2006). Disponible en: https://www.regjeringen.no/no/dokumenter/elektronisk-stem-megivning---utfordringer/id278479/
[74]ACE Project. Focus on E-voting. (ACE, 2011) disponible en http://aceproject.org/ace-en/focus/e-voting/about
[75]OSCE/ODIHR, NORWAY PARLIAMENTARY ELECTIONS 9 SEPTEMBER 2013 (Warsaw: OSCE, 2013); Institutt for samfunnsforskning, Internet Elections- What Do The Voters Think? (Oslo: Institutt for samfunnsforskning, 2014).

En la auditoría realizada por el tercero se encontraron algunos riesgos técnicos para mantener la integridad del software como la carencia de documentación y dificultades de acceso, además, algunos riesgos de la confidencialidad del voto dados por el sistema de generación de claves[76]. Otra situación que se recalcó fue la solución de problemas de programación hasta 5 días antes de los comicios, dificultando las auditorías[77]. En el caso del Centro Carter, se insistió en factores que escapaban a lo puramente técnico: la confidencialidad del voto se veía comprometida por los ambientes no controlados de la votación por internet -- muchos ciudadanos no entendían el sistema de votación--, y era necesario contar con una gran cantidad de experticia al interior del organismo de administración electoral[78]. En la auditoría estatal se mostraron algunos puntos buenos del sistema como su seguridad general, pero también se mostró cómo la votación no había funcionado para aumentar la votación juvenil y que los ciudadanos que votaban por internet eran los mismos que iban a votar por medios presenciales anteriormente[79]. De esta manera, en junio de 2014 el gobierno informó que los pilotos de votación por internet serían descontinuados teniendo en cuenta la presión política de la oposición ante algunos errores técnicos, el incumplimiento del objetivo de participación pactado y los costos requeridos.

El caso de Noruega muestra que cuando se realizan los adecuados procesos de transparencia y auditoría externa se puede evaluar objetivamente las necesidades, oportunidades y riesgos de la inclusión de tecnologías en las elecciones. Así, el organismo de administración electoral noruego decidió abandonar los pilotos de la votación por internet contando con diferentes puntos de vista y con los objetivos claros que llevaron a iniciar el uso de TICs. Igualmente, muestra que las tecnologías no deben tratar de igualar a la votación tradicional, sino superarla en sentido de seguridad, efectividad y sencillez.

Otro caso de transparencia que ha aportado a la adecuada implementación del voto electrónico en Europa ha sido la transparencia en Bélgica donde se invita a un grupo de expertos de las mejores universidades del país a auditar públicamente el aplicativo y las máquinas[80].

3.4 *Argentina, la crisis de la seguridad por oscuridad*

En Argentina es necesario hablar de dos historias de utilización de TICs en procesos electorales que revelan los problemas que conlleva la seguridad por oscuridad para la legitimidad de los procesos electorales. En primer lugar, tenemos la polémica que ha generado el software de escrutinio provisorio. Desde 1997, el organismo de administración electoral, a través de un concurso de proponentes, comisionó a la multinacional española Indra para programar y utilizar un software de escrutinio provisorio. Desde 2010, la multinacional se vio envuelta en una serie de escándalos en el mundo incluidos casos de corrupción en América Latina y fallos informáticos en España[81]. En julio de 2017, en una maniobra poco transparente, el organismo le entregó el control de todo el escrutinio provisorio a Indra a través del Correo Argentino ganando el concurso con solo un competidor[82]. Esta situación levantó muchas dudas sobre la confiabilidad del programa de Indra[83] y la oposición denunció un fraude realizado a través del software en las elecciones legislativas de 2017[84]. Por esto,

[76] Tor Bjørstad and Mnemonic, Technical Report Source Code Audit Of Norwegian Electronic Voting System (Oslo: Mnemonic, 2013).
[77] Teknisk Ukeblad, "Error In Encryption Of Email Voices", 2013, https://www.tu.no/artikler/feil-i-krypteringen-av-e-stemmer/234436.
[78] The Carter Center, Internet Voting Pilot: Norway'S 2013 Parliamentary Elections (Washington: The Carter Center, 2014).
[79] Institutt for samfunnsforskning, Internet Elections.
[80] NDI & IFES. Implementing and overseeing, 63.
[81] El Grillo, "Conozca Los Escándalos De Indra, La Empresa Encargada Del Conteo Electrónico En Las Próximas Elecciones", 2016, http://elgrillo.do/2016/05/conozca-los-escandalos-indra-la-empresa-cargo-del-conteo-electronico-las-proximas-elecciones/.
[82] La Política Online, "Confirmado: El Gobierno Le Dio A Indra El Control Del Escrutinio Provisorio", 2017, http://www.lapoliticaonline.com/nota/106363/.
[83] Infobae, "Piden Auditar El Escrutinio Provisorio Que Realizarán El Correo Argentino Y La Empresa INDRA", 2017, https://www.infobae.com/politica/2017/07/05/piden-auditar-el-escrutinio-provisorio-que-realizaran-el-correo-argentino-y-la-empresa-indra/.
[84] El Día, "El Kirchnerismo Siembra Sospechas Sobre El Escrutinio Electoral", 2017, http://www.eldia.com/nota/2017-10-10-2-29-54-el-kirchnerismo-siembra-sospechas-sobre-el-escrutinio-electoral-la-provincia.

el gobierno comisionó a la ONG Transparencia por Argentina para auditar el sistema. En el informe no se encontraron fallas de conteo, pero no se realizó un análisis del código fuente, ni de otros factores técnicos[85]. Asimismo, algunos medios levantaron serias dudas sobre la independencia de la ONG por tener tres contratos con el Estado y, por tanto, comprometer su independencia del gobierno[86].

En segundo lugar, tenemos el caso de la aplicación del voto electrónico en las provincias de Buenos Aires y Salta. En 2015, la votación electrónica se comenzó a usar en la Provincia de Buenos Aires en una concesión que se le entregó al Grupo MSA a través de su plataforma Vot. Ar. Así, apareció la Boleta Única Electrónica (BUE) un sistema de votación electrónica directa que entrega una boleta con un código para insertar en la urna y luego ser contado por otro dispositivo. En otras palabras, se contrasta la votación electrónica directa con los resultados de un conteo electrónico. De la misma forma, en 2016 se delegó el control de la votación en la Provincia de Salta a Vot.Ar. El sistema de BUE funciona por medio de seguridad por oscuridad, pues el código fuente del aplicativo le pertenece a la empresa y lo guarda celosamente. Sin embargo, a pesar de los comunicados que aseguraban la protección del código fuente, tanto en Buenos Aires como en Salta el código se filtró algunos días antes de las elecciones generales. Con esto, se comprometió todo el sistema de votación en dos provincias del país y se empezaron a levantar dudas sobre la seguridad del sistema.

Ante la falta de interés del organismo de administración electoral por realizar una auditoría independiente del sistema., varias organizaciones y oficinas del Estado pidieron auditar lo que estaba disponible, es decir, la máquina de votación directa y las boletas. En primer lugar, el Instituto Tecnológico de Buenos Aires realizó una auditoría contratado por la Defensoría del Pueblo. En los resultados se explican graves problemas técnicos de seguridad digital que hacían muy sencillo, con el conocimiento apropiado, intervenir los resultados de las elecciones[87]. En segundo lugar, la Fundación Vía Libre apoyada por la Fundación Heinrich Böll mostró graves problemas de seguridad digital, una total falta de transparencia, una carencia de comprensión del ciudadano común y los grandes costos que pueden implicar construir un sistema de votación electrónica seguro[88]. Finalmente, algunos técnicos decidieron probar la seguridad informática de las máquinas encontrando un sistema secundario que podía guardar información sobre el votante y una posible vía de infiltración en la parte trasera de la máquina[89].

El caso argentino muestra como no contar con los mecanismos de transparencia adecuados y, por el contrario, construir la seguridad del software basada en el desconocimiento de los actores, puede poner en riesgo el desarrollo de las elecciones democráticas y levantar importantes dudas sobre el proceso electoral. En ningún caso, la seguridad de un sistema informático debe basarse en que las personas desconozcan el sistema, pues, como muestran las filtraciones de partes de los sistemas de votación electrónica, los atacantes pueden encontrar fácilmente la información requerida[90]. Así pues, Colombia debe tratar de tener sistemas transparentes y cuya seguridad está basada en la robustez del aplicativo, mas no en supuestos poco realistas sobre la posibilidad de negar el acceso a la información.

Implementar correctamente un sistema electoral que incluya TIC en el proceso es una actividad compleja que

[85]Iprofesional, "Advierten Que La Etapa Informática Del Escrutinio De Las Elecciones Del Domingo Es "Una Gran Caja Negra"", 2017, http://www.iprofesional.com/notas/257449-software-provincia-de-buenos-aires-gobierno-elecciones-kirchnerismo-computadora-correo-argentino-Advierten-que-la-etapa-informatica-del-escrutinio-de-las-elecciones-del-domingo-es-una-gran-caja-negra?page_y=0.
[86]El Disenso, "Opacidad Electoral: Le Pagaron A Un Empleado Del Ministerio Del Interior Para Que Audite El Escrutinio Provisorio Desde Su ONG", 2017, http://www.eldisenso.com/politica/opacidad-electoral-frigerio-le-pago-empleado-suyo-audite-escrutinio-provisorio-indra-desde-una-ong/.
[87]Defensoría del Pueblo de la C.A.B.A., DVT 56-504: Auditoría De Sistema De Votación Electrónica 2015 Para La Defensoría Del Pueblo De La C.A.B.A. (Buenos Aires: CABA, 2015).
[88]Beatriz Busaniche, Voto Electrónico Una Solución En Busca De Problemas (Buenos Aires: Fundación Vía Libre & Heinrich Böll, 2017).
[89]https://hackingthesystem4fun.blogspot.de/2015/07/el-sistema-oculto-en-las-maquinas-de.html
[90]La Nación, "Filtran Parte Del Código Fuente De La Boleta Electrónica Porteña", 2015, http://www.lanacion.com.ar/1803251-filtran-parte-del-codigo-fuente-de-la-boleta-electronica-portena.
La Nación, "Filtran El Software De Control De Una Máquina De Voto Electrónico Usada En Salta", 2017, http://www.lanacion.com.ar/2054577-filtran-el-codigo-de-una-maquina-de-voto-electronico-de-salta-y-alertan-sobre-los-riesgos-del-sistema.

debe incluir la transparencia como eje central y, por tanto, garantizar la auditoría por cualquier persona interesada. La Ley Estatutaria 1475 de 2011 en su artículo 45 tiene una disposición que permite desarrollar esta buena práctica, a pesar de los problemas para hacerlo, la Registraduría debe hacer cambios sustanciales en la forma como le da aplicación a esta norma y con ello empezar a abrir la caja negra en que se ha convertido el software electoral en Colombia.

4 Propuesta de pruebas para la auditoría

Una auditoría para un sistema informacional busca determinar si éste es robusto, confiable, seguro y realiza exclusivamente las operaciones y funciones para las cuales fue diseñado, de acuerdo al análisis y diseño, garantizando la integridad en el procesamiento de toda la información. Igualmente, una auditoría es un proceso complejo --directamente relacionado con la complejidad y tamaño del sistema que se va a analizar-- que requiere de muy diferentes experticias, tiene diferentes niveles y requiere de un plazo de tiempo considerable para ser realizado. No hay una fórmula única para las auditorías aunque sí existen buenas prácticas comunes.

Con base en la Ley Estatutaria 1475 de 2011 los partidos políticos y la Misión de Observación Electoral (MOE) están facultados legalmente para auditar el sistema electoral del país y con ello aportar a fortalecer la confianza en el proceso. El sistema que se propone auditar corresponde a uno de los que utiliza el Estado colombiano en sus procesos electorales. Desafortunadamente, aunque las actividades de información, preconteo, escrutinio y digitalización son cuatro actividades diferentes dentro del proceso electoral y el sistema informacional no refleja esas diferencias completamente, hay apartes del sistema que están interrelacionados. La RNEC hace un único contrato para las cuatro actividades que además incluye el recurso de personal y su capacitación. Con fundamento en lo anterior, se puede afirmar que las elecciones en Colombia están completamente tercerizadas, es decir, privatizadas. De acuerdo con el contrato el Estado colombiano hace una supervisión de su ejecución y debe documentar este proceso, pero toda la ejecución está a cargo del (los) contratista (s).

Es decir, no solo el sistema es complejo, sino que es muy difícil decir que se va a auditar tan solo la actividad de escrutinio, al final se puede intentar concentrar el esfuerzo en lo relacionado con escrutinio pero la mayor parte de las veces se estará auditando al sistema como tal. De hecho, el propio contrato no es claro sobre los documentos y parece pedirlos solo para unas actividades (ej: preconteo) y no para otras

(escrutinio). Sin embargo, esto no tendría sentido y si el sistema que se usa es el mismo para las diferentes actividades lo que se pide para la actividad de preconteo servirá para la de escrutinio también. Por esto, para la elaboración de este documento se consideró el contrato y el sistema como un todo.

Además de las complejidades descritas, la auditoría que se propone realizar (art. 45 Ley Estatutaria 1475 de 2011) enfrenta otra situación problemática que son las restricciones que se han planteado para este primer ejercicio de auditoría:

1. La Registraduría tan solo ha manifestado que se pondrá a disposición de los auditores una terminal de las usadas por el sistema para que sea auditada durante una semana previa a las elecciones.
2. La inminencia de los comicios electores en Colombia (marzo y mayo de 2018) obligan a pensar que los recursos --humanos, financieros y técnicos disponibles para hacer esta auditoría serán reducidos.

Es necesario poner de presente en este punto que aún si el nivel de auditoría es superficial es posible que se identifiquen problemas sustanciales. Resulta, por lo tanto, fundamental que como sociedad se plantee que en caso de encontrar vulnerabilidades sustanciales será necesario actuar frente a ellas. Es decir, se debe reconocer que los resultados pueden comprometer el proceso electoral. Esto es especialmente grave si se considera que no habrá plazo para mitigar o corregir las irregularidades que se puedan identificar.
Teniendo como base el análisis del contrato entre la Registraduría y el contratista para las elecciones de 2018, el presente documento ofrece un punto de partida para un ejercicio de auditoría que se ve reflejado en una serie de pruebas de seguridad básica en forma de checklist sobre los equipos de escrutinio, posteriormente plantea los recursos documentales base con que se debería contar para hacer una auditoría y que debe servir en forma de checklist para realizar una comprobación inicial del cumplimiento documental frente a los requisitos contractuales. Posteriormente plantea las pruebas funcionales a realizar sobre el software de escrutinio y explica los tres escenarios ideales de auditoría que se han identificado clasificados por su nivel de profundidad respecto del sistema --se presenta en una suerte de módulos que se van agregando para ir más profundo en el análisis correspondiente--. Finalmente, se plantean las opciones que consideramos más viable para desarrollar considerando las restricciones de tiempo y recursos disponibles para hacer este ejercicio en 2018.

En suma, con base en el análisis realizado consideramos que como mínimo el alcance de una eventual auditoría para el software de escrutinio en 2018 debería poder abarcar el levantamiento de información documental, las pruebas de los checklist de seguridad básica y pruebas funcionales. La calidad y profundidad del análisis, así como la inclusión de otras pruebas dependerán de los recursos y el tiempo disponible para la realización de la auditoría.

4.1 *Checklist #1. Pruebas básicas de seguridad*

Con el propósito de verificar la seguridad de los sistemas donde se realizan los escrutinios es necesario establecer su nivel base de seguridad. Esto se realiza mediante una verificación tipo checklist que busca medir el aseguramiento de un equipo frente a las buenas prácticas de seguridad.

4.1.1 Pruebas generales:

1. ¿El chasis se encuentra dentro de un contenedor seguro?
2. ¿El chasis cuenta con sellos de seguridad para demostrar si ha sido abierto?
3. ¿El chasis cuenta con puertos USB?
4. ¿El chasis cuenta con puertos firewire?
5. ¿El chasis cuenta con puertos eSATA?
6. ¿El chasis cuenta con el sticker de licenciamiento de windows?
7. ¿Qué versión de windows corresponde al sticker?
8. ¿El teclado es usb?
9. ¿Cuántos dispositivos usb se encuentran conectados al equipo?
10. Fotografiar todos los dispositivos usb conectados al equipo
11. Fotografiar todos los demás dispositivos conectados al equipo
12. Listar puertos encontrados en el chasis.
13. ¿El equipo cuenta con cámara integrada?
14. Fotografiar el chasis
15. ¿Cuál es la marca del equipo?
16. ¿Cuál es el serial del equipo?
17. ¿Cuál es el modelo del equipo?
18. ¿Cuáles son las especificaciones de hardware del equipo?

- ***a.*** Board
- ***b.*** Procesador
- ***c.*** Memoria
- ***d.*** Disco duro
- ***e.*** Unidades ópticas
- ***f.*** Interfaces de red
- ***g.*** Otros

19. Revisar si el equipo cuenta con clave de acceso al BIOS.
20. ¿La fecha y hora están correctas al arrancar el equipo?
21. Revisar si el equipo permite su arranque desde dispositivos removibles (USB; CD; DVD, etc.).
22. Revisar si el equipo permite su arranque desde elementos de red.
23. ¿Cuál es el orden de boot establecido en el computador?
24. ¿Se puede modificar el orden?
25. ¿La unidad de disco se encuentra cifrada?
26. Revisar si el procesador intel es vulnerable a specter y meltdown[91].

4.1.2 Pruebas con usuario administrador

27. ¿La fecha y hora están correctas en el sistema operativo, incluyendo la zona horaria?
28. Ejecutar el aplicativo microsoft baseline security analyzer[92].
29. Volcar políticas de directiva de grupo y de seguridad aplicadas al usuario y equipo.

- ***a.*** Usar comando: gpresult

30. ¿Qué versión de windows está instalada en el equipo?

- ***a.*** Usar el comando: winver

31. ¿El equipo se encuentra correctamente licenciado?
32. ¿Cuál es la fecha de instalación del sistema operativo?

- ***a.*** Usar el comando: systeminfo

33. ¿Cuál es la fecha de la última actualización del sistema operativo?

- ***a.*** Usar comando powershell: Get-Hotfix

34. ¿El sistema operativo está al día de actualizaciones?
35. ¿El computador se encuentra dentro de un dominio de windows?
36. Listar aplicativos instalados.
37. Listar usuarios locales y anotar fecha de último cambio de credenciales, si están activos.
38. Listar usuarios administradores locales y anotar fecha de último cambio de credenciales, si están activos.
39. Listar grupos locales y sus miembros.
40. Listar política de contraseñas del equipo.
41. Listar servicios activos.
42. ¿El firewall está activo?
43. ¿El equipo cuenta con el servicio de escritorio remoto activo?
44. ¿El equipo cuenta con el servicio de carpetas com-

[91] https://www.intel.com/content/www/us/en/support/articles/000025619/software.html
[92] https://www.microsoft.com/en-us/download/details.aspx?id=7558

partidas activo?
45. ¿El equipo cuenta con carpetas compartidas?
46. ¿Cuenta con antivirus?
47. ¿El antivirus está actualizado?
48. ¿La funcionalidad de windows script host está activa?
49. ¿La funcionalidad de UAC está activa?
50. ¿El protocolo WPAD está activo?
51. ¿El protocolo LLMNR está activo?
52. ¿El protocolo Windows browser protocol está activo?
53. ¿El protocolo NetBIOS está activo?
54. ¿El protocolo WDigest está activo?
55. ¿El protocolo SMBv1 está activo?
56. ¿El equipo cuenta con el aplicativo EMET instalado?
57. ¿El equipo cuenta con la herramienta applocker instalada?
58. ¿El equipo cuenta con software de correo electrónico instalado?
59. ¿El equipo cuenta con cuentas de correo electrónico configuradas?
60. ¿El equipo cuenta con software de mensajería instantánea?
61. ¿El equipo cuenta con navegadores de internet?
a. ¿Cuáles son sus versiones?
b. Listar complementos instalados en los navegadores
62. Revisar historial de navegación de todos los navegadores y listar sus entradas
63. ¿El equipo cuenta con software de ofimática?
a. ¿Cuáles son sus versiones?
64. ¿El equipo cuenta con Adobe Acrobat?
a. ¿Cuáles son sus versiones?
65. ¿El equipo cuenta con Adobe Flash?
a. ¿Cuáles son sus versiones?
66. ¿El equipo cuenta con Oracle JAVA SE, JDK o JRE?
a. ¿Cuáles son sus versiones?
67. ¿Cuántos usuarios se han logueado en el equipo?
a. Revisar perfiles creados en el disco del equipo.
68. ¿El equipo cuenta con software de administración remota?
69. ¿El equipo permite el uso de memorias o discos usb?
70. ¿El equipo permite el uso de tarjetas de red usb? (Probar tarjetas wifi, bluetooth y módem 2g-3g-4g)
71. ¿El equipo equipo puede visualizar redes inalámbricas wifi?
72. ¿El equipo equipo puede visualizar redes inalámbricas bluetooth?
73. ¿El equipo permite navegar en internet?
74. ¿El uso de internet está limitado?
75. ¿El equipo permite el uso de aplicativos portables?[93]
76. ¿La sesión se bloquea de forma automática?
a. ¿En cuanto tiempo?
77. ¿La cámara web es funcional? (Si existe)
78. ¿El micrófono es funcional? (Si existe)
79. ¿Se puede navegar el sistema de archivos?
80. ¿Se puede cambiar la fecha y hora del equipo?
81. ¿Se puede abrir la consola de comandos cmd?
82. ¿Se puede abrir la consola de comandos powershell?
83. ¿Se puede abrir la consola de comandos powershell_ise?
84. ¿Se puede abrir el editor de registro regedit?
85. ¿Se puede abrir el panel de control?
86. ¿Se puede abrir el administrador de tareas?
87. ¿Se pueden instalar aplicativos en el equipo?
88. ¿Se pueden desinstalar aplicativos del equipo?
89. ¿Se pueden crear usuarios en el equipo?

4.1.3 Pruebas con usuario no administrador (El utilizado para usar el sistema)

90. ¿El equipo permite el uso de memorias o discos usb?
91. ¿El equipo permite el uso de tarjetas de red usb? (Probar tarjetas wifi, bluetooth y módem 2g-3g-4g)
92. ¿El equipo equipo puede visualizar redes inalámbricas wifi?
93. ¿El equipo equipo puede visualizar redes inalámbricas bluetooth?
94. ¿El equipo permite navegar en internet?

[93] https://portableapps.com/

95. ¿El uso de internet está limitado?
96. ¿El equipo permite el uso de aplicativos portables?[94]
97. ¿La sesión se bloquea de forma automática?
a. ¿En cuánto tiempo?
98. ¿La cámara web es funcional? (Si existe)
99. ¿El micrófono es funcional? (Si existe)
100. ¿Se puede navegar el sistema de archivos?
101. ¿Se puede cambiar la fecha y hora del equipo?
102. ¿Se puede abrir la consola de comandos cmd?
103. ¿Se puede abrir la consola de comandos powershell?
104. ¿Se puede abrir la consola de comandos powershell_ise?
105. ¿Se puede abrir el editor de registro regedit?
106. ¿Se puede abrir el panel de control?
107. ¿Se puede abrir el administrador de tareas?
108. ¿Se pueden instalar aplicativos en el equipo?
109. ¿Se pueden desinstalar aplicativos del equipo?
110. ¿Se pueden crear usuarios en el equipo?

Eventualmente si se quisiera realizar una prueba profunda de seguridad, esta tendría que abarcar no solo los equipos utilizados para el proceso de escrutinio, sino también, todas las infraestructuras relacionadas con el sistema electoral. Para ello hay estándares internacionales como las revisión del GAP 27001 y las pruebas de seguridad planteadas por el proyecto OWASP[95].

4.2 Recursos documentales base para la auditoría

La propuesta de la Unión Temporal sobre el proceso de Selección abreviada 010 de 2017- RNEC y sus pliegos de condiciones y anexos cuenta con unos requisitos claramente identificados por las partes. Con la finalidad de auditar el proceso electoral, los mínimos recursos documentales con que se debería contar es con el acceso a todos los entregables del contratista así como los análisis de riesgos preliminares y los resultados de la labor de auditoria e interventoria sobre la ejecución del contrato.

Con base en la documentación de proceso, se presenta el siguiente listado de documentos requeridos que deben ponerse a disposición del equipo auditor.

El siguiente listado se puede considerar un checklist de documentación requerida contractualmente para el cumplimiento de los pliegos de contratación. Inicialmente se debe realizar una matriz con los documentos y establecer si existen o no y si son compartidos o no con el equipo auditor.

4.2.1 Software

- Versión definitiva del software de escrutinio con datos de prueba (DIVIPOL y candidatos).
- Código fuente del software que se utiliza para el sistema.

4.2.2 Documentales[96]

- Diseño tecnológico de la solución.
- Modelo técnico de la solución.
- Esquema para el manejo de la seguridad informática implementado por el contratista.
- Diseño, mapa de red e informes del sistema de monitoreo de la red por CPD-CCS[97].

[94] https://portableapps.com/
[95] https://www.owasp.org/index.php/Main_Page
[96] Contrato de prestación de servicios No. 055 de 2017, suscrito entre la Registraduría Nacional del Estado civil y Unión temporal soluciones informáticas electorales 2018. "UT SIE 2018".p 5. Cláusula tercera. Capítulo 1. Alcance: "Para la prestación del servicio, EL CONTRATISTA deberá proveer a la Registraduría Nacional del Estado Civil de una solución informática enfocada a la calidad del servicio, con procedimientos y gestión de riesgos debidamente documentados."
[97] Ibid. p. 11 "deberá disponer de un sistema de monitoreo y análisis del tráfico de la red de datos LAN en cada Centro de Procesamiento (CPD/CCR), monitoreo a los servidores y equipos de procesamiento en cuanto a rendimiento y nivel de disponibilidad de procesamiento y almacenamiento en memoria principal"

- Diseño, mapa de red e informes del sistema de monitoreo de las bases de datos por CPD-CCS.
- Diseño, mapa de red e informes del sistema de monitoreo de los servidores por CPD-CCS.
- Política de calidad.
- Manual de procesos y procedimientos.
- Listado maestro de documentos del sistema de calidad.
- Procedimiento de gestión de riesgos.
- Metodología de gestión de riesgos.
- Análisis de riesgos.
- Planos de redes de datos y eléctricas por CPD-CCR y salas de prensa[98].
- Infraestructura instalada y su capacidad por CPD-CCR y salas de prensa.
- Arquitectura dispositivos de seguridad informática y demás elementos instalados por la registraduría en los CPD[99].
- Organigrama y autorizaciones para la ejecución del proyecto de cada CPD-CCR[100].
- Plan de capacitación del personal asignado al proceso electoral.
- Plan de capacitación del personal sobre el proceso y protocolo a emplear para la transmisión-recepción de datos electorales a los transmisores y receptores contratados.
- Materiales utilizados en el plan de capacitación.
- Procedimiento de generación de backups.
- Protocolo de comunicaciones.
- Formatos de Recepción Telefónica.
- Documentación de la herramienta tecnológica que permita llevar un control de tiempo de la información de las mesas transmitidas y recepcionadas.
- Documentación de la herramienta tecnológica o procedimientos que permitan medir el desempeño de los transmisores y receptores durante la capacitación, pruebas y simulacros.
- Documentación de los canales de datos y de la seguridad informática requerida para la transmisión de datos electorales al Centro de Consolidación Nacional y entre los CPD's con los CCR's y con las salas de prensa.
- Documentación sobre la configuración del registro de logs de auditoría de aquellas transacciones que afecten la base de datos (inclusiones, correcciones), indicando nombre de la estación, usuario, fecha y hora.
- Documentación licencias del software especializado para realizar el procesamiento de información de datos electorales de preconteo o el registro de derechos de autor del mismo.
- Metodología de programación de software.
- Manual o procedimiento de programación segura de software.
- Manual de pruebas funcionales, no funcionales unitarias y de carga-stress de software.
- Política de seguridad de la información de la unión temporal.
- Política de tratamiento de datos personales de la unión temporal.
- Política de manejo y atención de incidentes informáticos.
- Licenciamiento de base de datos.
- Licenciamiento Antivirus.
- Licenciamiento servidores y estaciones de trabajo.
- Procedimiento para evaluar y calificar la calidad de la información procesada.
- Plan de Continuidad del proceso[101].
- Plan de Contingencia del Proceso.
- Manuales de Sistema.
- Manuales de usuario.
- Documentación de funciones por cargo y roles.
- Documentación de procedimientos por actividades.
- Documentación de mapa de riesgos y planes de continuidad y de contingencia.

[938] Ibid. p 20. "planos de la red de datos y eléctrica, así como la documentación pertinente a la infraestructura instalada y su capacidad."
[99]Ibid. p 8. "EL CONTRATISTA deberá establecer dentro de los Centros de Procesamiento (CPD/CCR), específicamente en los rack de comunicaciones, el espacio requerido para que la Registraduría Nacional del Estado Civil instale los equipos de comunicaciones, dispositivos de seguridad informática y UPS's que ésta disponga para de la red nacional electoral."
[100]Ibid P. 9. "deberá presentar el organigrama para la ejecución del proyecto en cada Centro de Procesamiento (CPD/CCR), el cual deberá especificar la cantidad y ubicación del recurso humano que proporcionará dentro del servicio para los siguientes roles, de conformidad con el estudio previo, el pliego de condiciones definitivo y la propuesta presentada por EL CONTRATISTA los cuales forman parte integral del presente contrato."
[101]Ibid. P. 18. "L CONTRATISTA para el procesamiento electrónico de datos electorales de preconteo deberá disponer de un procedimiento - Plan de Continuidad del proceso- para atender las diferentes situaciones que impidan el normal funcionamiento de cada CPD, el cual deberá estar documentado, soportado y socializado.

- Documento del esquema de administración y seguimiento a las actualizaciones del software y sus versiones.
- Especificaciones técnicas del IDS, Firewall y sistema de almacenamiento.

4.2.3 Certificaciones

- Certificaciones de estado de la Registraduría frente a los CPD, CCR y salas de prensa
- Certificación acometidas eléctricas realizado por firma especializada por cada CPR-CCR y salas de prensa[102].
- Certificación del cableado eléctrico realizado por firma externa por cada CPR-CCS y salas de prensa[103].
- Certificado cableado estructurado realizado por firma especializada por cada CPR-CCR y salas de prensa[104].
- Certificación que avale el datacenter principal como tier-2.
- Certificación del datacenter secundario o alterno.
- Certificación seguridad informática perimetral.
- Certificación de una empresa especializada en pruebas de rendimiento y seguridad informática sobre las soluciones informáticas.
- Certificación no vulnerabilidad de la solución.

4.2.4 Resultados de auditorías internas y externas

- Informe auditoría interna al sistema de calidad.
- Informe auditoria realizado por la empresa especializada sobre software.
- Pruebas de carga sobre UPS por CPD-CCR y salas de prensa.
- Prueba de carga plantas eléctricas por CPD-CCR y salas de prensa.
- Pruebas sistema de monitoreo de red por CPD-CCR y salas de prensa.
- Pruebas de vulnerabilidades y plan de mitigación[105].
- Resultados de la prueba técnica de funcionalidad.
- Resultados primer y segundo simulacro para las elecciones al congreso.
- Pruebas sobre el procedimiento de generación de backups.
- Pruebas sobre sistema OCR para asegurar el porcentaje de error menor del 0.1%[106].
- Pruebas funcionales del software especializado para realizar el procesamiento de información de datos electorales de preconteo.
- Pruebas no funcionales del software especializado para realizar el procesamiento de información de datos electorales de preconteo.
- Pruebas unitarias del software especializado para realizar el procesamiento de información de datos electorales de preconteo.
- Pruebas de aceptación del software especializado para realizar el procesamiento de información de datos electorales de preconteo.
- Pruebas de carga y stress del software especializado para realizar el procesamiento de información de datos electorales de preconteo.
- Pruebas del plan de continuidad del proceso.
- Pruebas del plan de contingencia del proceso.
-

4.2.5 Actas

- Actas de aprobación de los centros de Procesamiento (CPD/CCR)[107].
- Actas de verificación de cumplimiento requerimientos técnicos por cada CPD-CCR[108].

[102]Ibid. P. 7 "se verificará y certificará el estado de los Centros de Procesamiento (CPD/CCR)"
[103]Ibid. P. 19 "deberá garantizar que las acometidas eléctricas (normal y regulada) se encuentren en perfecto estado y con la capacidad suficiente para soportar la infraestructura ofrecida a plena carga en los Centros de Procesamiento (CPD/CCR). Para ello, deberá entregar una certificación expedida por una firma especializada"
[104]Ibid P. 8. "deberá garantizar que el cableado eléctrico sea certificado por una firma externa en cuanto a su instalación y capacidad de los circuitos en general."
[105]Ibid P. 13. "EL CONTRATISTA deberá entregar el resultado del diagnóstico de vulnerabilidades y el plan de mitigación con la debida antelación a la realización de las pruebas correspondientes, este requerimiento será verificado por la Registraduría Nacional del Estado Civil o quien esta designe."
[106]Ibid. P. 15. "EL CONTRATISTA deberá asegurar un porcentaje de error inferior al 0.1% de las cifras interpretadas y verificadas."
[107] Ibid. P. 7. "Las instalaciones locativas dispuestas por EL CONTRATISTA, en cada departamento, para el funcionamiento de los Centros de Procesamiento (CPD/CCR), deberán ser aprobadas previamente por la Gerencia de Informática."
[108]Ibid P. 41. "La Supervisión del contrato verificará que EL CONTRATISTA cumpla con los requerimientos técnicos descritos anteriormente"

- Actas de aprobación de las salas de prensa.
- Actas de capacitaciones del personal asignado al proceso electoral.
- Actas de capacitaciones sobre el proceso y protocolo a emplear para la transmisión-recepción de datos electorales a los transmisores y receptores contratados
- Actas de aprobación de servidores de todos los sistemas[109].
- Acta de verificación de la solución informática de todos los sistemas.

4.3 Pruebas de funcionalidad

Con la finalidad de comprobar el funcionamiento del software se debe realizar una prueba de sus funcionalidades principales. A continuación, se presenta una lista de chequeo de las pruebas mínimas a realizar según lo especificado en los pliegos de condiciones del contrato celebrado.

4.3.1 Desarrollo de la prueba

1. ¿Dispuso el oferente de una infraestructura de computadores independientes o conectados a nivel de red de área local para el desarrollo de la prueba? (Especificar).
2. ¿Se realizó el proceso de configurar el tipo de escrutinio (Auxiliar, Municipal y General)?
3. ¿Permitió configurar la comisión escrutadora: Enrolar mediante el empleo de captor de huellas, autenticar y asignar claves a los miembros de Comisión Escrutadora y claveros?
4. ¿Se verificó que el sistema tiene algún mecanismo de respaldo en caso tal de no ser posible la autenticación biométrica de algunos o todos los miembros de la comisión escrutadora y clavero previamente enrolados?
5. ¿Se verificó que el software permite la modificación de datos relacionados con integrantes de las comisiones escrutadoras, claveros y que registra el cambio en el Acta General de escrutinio y en los logs del sistema?
6. ¿Se verificó que el software permite el registro de los testigos políticos, apoderados y entes de control que se hacen presentes en el escrutinio; al igual que las observaciones por ellos realizadas, las cuales aparecen en el Acta General de escrutinio?
7. ¿Se verificó que el software genera e imprime el acta de entrega del mismo, una vez se realiza el proceso de configuración? Se verificó que el software permite el registro de los testigos políticos, apoderados y entes de control que se hacen presentes en el escrutinio; al igual que las observaciones por ellos realizadas, las cuales deben aparecer en el Acta General de escrutinio?
8. ¿Se verificó que el aplicativo permite el registro de observaciones o novedades que surgen durante el proceso del escrutinio y se verificó que están contenidas en el Acta General de escrutinio?
9. El aplicativo permite escoger la corporación a escrutar en cualquier orden?
10. ¿El aplicativo permite escoger la zona, puesto y mesa a escrutar en cualquier orden?
11. ¿El aplicativo permite capturar el total de sufragantes, el estado de los sobres, términos de introducción, cantidad de firmas del acta de escrutinio (E-14) y si este contiene enmendaduras o tachaduras?
12. ¿El software permite la captura de las votaciones registradas en las actas de escrutinio de los jurados de votación (E-14) por cada uno de los candidatos o listas, partidos o movimientos políticos, grupos significativos de ciudadanos, votos en blanco, nulos y no marcados; lo anterior, como un proceso previo a grabar la información capturada?

[109] Ibid. P. 43 "La configuración de los servidores estará sujeta a la revisión y aprobación por parte de la supervisión del contra

13. ¿El aplicativo en las instancias de los escrutinios auxiliares y municipales cada vez que se va a grabar o escrutar una mesa, visualiza una opción que indica si hubo o no recuento de votos?
14. ¿El aplicativo permite capturar las reclamaciones y solicitudes de recuento de votos en concordancia con el código electoral?
15. ¿El aplicativo permite responder las solicitudes del recuento de votos, reclamaciones al escrutinio y reclamaciones a una mesa en particular?
16. ¿El aplicativo genera las resoluciones con las cuales se resuelven los diferentes recursos o apelaciones?
17. ¿El software permite la consolidación de los resultados?
18. El software genera backups de manera automática cada 5% de mesas grabadas, sin que se afecte o se detenga el desarrollo del proceso de escrutinio. Lo anterior debe quedar registrado en el log de auditoría.
19. ¿El aplicativo permite visualizar el avance del escrutinio indicando la cantidad de mesas instaladas, leídas, faltantes y los porcentajes de mesas escrutadas?
20. ¿El aplicativo permite realizar recesos de escrutinio?
21. El hecho de generar un receso en el escrutinio ¿Queda registrado en el log de auditoría y en el Acta General de escrutinios?
22. ¿El aplicativo permite generar en medio impreso informes parciales, con marca de agua, de los reportes E-24 y E-26, disgregados por mesas, zonas, puestos o municipios, según el tipo de escrutinio?
23. ¿El aplicativo genera el total de votos por cada una de las listas de candidatos en contienda con los formularios E-24 y E-26?
24. ¿El aplicativo solicita la autenticación y claves a cada uno de los miembros de la comisión escrutadora, al momento de ingresar al sistema, al restituir o modificar una contraseña, al modificar una mesa y al generar reportes de E-24, E-26, actas y resoluciones?
25. ¿El aplicativo guarda el rastro de auditoría de todos y de cada uno de los registros que se adiciona o se modifican en la base de datos, indicando fecha y hora?
26. ¿El Acta General de escrutinio es editable en todos sus campos?
27. ¿El aplicativo permite el cierre de los escrutinios auxiliares y municipales generando el backup, los reportes, archivos necesarios a cargar en las comisiones Municipales y Departamentales respectivamente?
28. ¿El aplicativo genera la información de los escrutinios en medio magnético, discriminada por mesa, puesto, zona, Municipio y Departamento?

4.3.2 *Reportes*

1. ¿El aplicativo permite la generación e impresión de un informe de correcciones y modificaciones, mostrando información relacionada con las modificaciones realizadas a las mesas escrutadas?
2. ¿El aplicativo permite la generación e impresión de un informe mostrando las mesas en cero?
3. ¿El aplicativo permite la impresión del log de Auditoría del proceso o sistema?
4. ¿El sistema permite la impresión del E-24, E-26 Y Acta General de Escrutinio?

4.3.3 *Escrutinio general (Departamental)*

1. ¿El sistema permite el cargue de los archivos municipales?
2. ¿En el escrutinio departamental el E-24 está totalizado por municipio?
3. ¿El sistema permite hacer la declaratoria de elección de Cámara Departamental de San Andrés?

4.3.4 *Consideraciones generales para las pruebas de funcionalidad*

- Las pantallas de captura de datos deben estar diseñadas en forma consistente con los documentos de los manuales.
- En el ingreso de los datos, la aplicación deben tener mensajes de ayuda, con el fin de facilitar la captura de la información.
- El sistema debe restringir el acceso de los usuarios a las diferentes opciones de la aplicación que

no correspondan con su perfil dentro del sistema.
- Verificar los procedimientos de asignación de permisos a usuarios de la base de datos.
- Verificar en cada pantalla de captura, que los campos de los datos importantes sean de obligatoria digitación.
- En toda la aplicación, cada campo deben tener el formato de datos apropiado (impedir digitar caracteres en capturas numéricas, evitar números decimales donde se espera solo enteros, imposibilidad de ingresar números negativos, etc.).
- Para los campos numéricos y campos fecha, tengan controles de límite.
- En la captura o modificación de datos críticos tengan una pista (log o bitácora) donde se identifique lo siguiente: nombre del usuario, fecha y hora, valor del campo y donde se realizó la transacción así como qué tipo de operación realizó ese cambio.
- Registro de accesos al sistema.
- Registro de número de intentos fallidos de acceso.
- Verificar que los log de la aplicación puedan ser revisados por los responsables para investigar accesos y manipulaciones no autorizadas.
- Verificar que existen mecanismos para realizar un monitoreo del avance de digitalización y captura (Reportando tiempos en el proceso, avances y faltantes).
- Verificar que los datos ingresados no puedan ser re-ingresados para el procesamiento más de una vez. También se debe verificar el control de la integridad de la transmisión de datos con el uso de firma electrónica o método equivalente sobre las actas digitalizadas).
- Si en el ingreso de los datos hay un rechazo por el sistema; que ese dato sea analizado y corregido por los usuarios. (Comprobar la integridad de las actas, en caso de no coincidir no debería permitir avanzar el proceso. En el caso de la captura, las actas deben pasan por dos procesos para realizar la captura y la validación).
- Validar los procedimientos de excepciones tales como: una acta tenga problemas de origen, Como datos ilegibles, etcétera. (Si el número es ilegible, el que escribe la información tiene la responsabilidad de escribir el número que está escrito con texto. Si la acta no es legible por errores de digitalización, esto es, la imagen no es lo suficientemente clara para determinar los números, es responsabilidad de quien digitaliza marcarla como acta ilegible y se regresa el acta para que se digitalice nuevamente).
- Revisar el funcionamiento del procedimiento del validador al momento que se detecte que un error de captura.
- Asegurar la consistencia de los datos de las transacciones en la base de datos local y en las bases de datos de replicación. (Se verificó el entorno de base de datos y la replicación a dos bases de datos, una en sitio y otra fuera en la central, se realizaron consultas para verificar la consistencia de las réplicas de información).
- Asegurar que existan mecanismos de detección de errores y de prácticas de corrección de los mismos. (Por ejemplo, el personal de supervisión de captura llevaba registro de los errores detectados en el sistema y posteriormente se reportaban al equipo de desarrollo para su atención)
- Mantener continuidad en el procedimiento en línea en caso de inoperatividad de alguna terminal.
- Verificar la existencia de manuales y procedimientos de entrenamiento.
- Minimizar la posibilidad de que se cometan errores humanos durante la captura de datos. (El sistema no permite que se introduzcan datos erróneos dentro de ciertos parámetros, minimizando de esta forma que se cometan errores humanos durante la captura de estos. Los campos de captura, los botones y otros elementos de la interfaz de las aplicaciones tienen el tamaño suficiente, así como una distribución adecuada).
- Restringir la posibilidad de ingresos de datos, consulta y actualización de archivos a personas exclusivamente autorizadas e identificadas. (Manejo de contraseñas y por medio de control de acceso tanto físico como lógico a los equipos y sistemas).
- Asegurar el mantenimiento confidencial de las claves de cifrado de datos y contraseñas.

- Facilitar y simplificar la tarea del operador.
- Asegurar, que el sistema sea utilizado por operadores autorizados y desde lugares autorizados.
- Asegurar la autenticidad del operador/usuario.
- Evitar que personas no autorizadas puedan obtener información confidencial.
- Verificar que existan procedimientos para el control de cambios y de versiones.
- Comprobar que el sistema tenga el licenciamiento requerido para su operación.
- Pruebas de estrés a las aplicaciones que se utilicen en el sistema.

5 Posibles escenarios para una auditoría al sistema de escrutinio de las elecciones en Colombia

Para presentar diversos escenarios de auditoría que nos permitan ir de lo más básico a lo más complejo describimos los tres tipos diferentes de auditoría que se categorizan según el objeto de la evaluación:

1. Auditoría documental

Como su nombre lo indica lo que se busca analizar en este caso es los documentos que dan cuenta de la ejecución del contrato y de su revisión y seguimiento. Es mucho lo que se puede aprender de un sistema tan sólo analizando los requerimientos que el contratante hizo, la descripción que del mismo hacen sus fabricantes, las características que tiene, las versiones que dicen implementar, etcétera. Igualmente, se puede conocer bastante de las auditorías que se han hecho donde seguramente y se podrá saber sobre los problemas identificados y las soluciones implementadas. Adicionalmente, conocer las certificaciones con que cuenta y las que le faltan también puede servir para darse una idea de sus fortalezas y debilidades. Para esto, se evaluarían los documentos que se han descrito más arriba como documentos mencionados y exigidos en el propio contrato.
Esta auditoría puede fortalecerse con un análisis de calidad que use como referencia las normas ISO 9001.

2. Pruebas de seguridad

Hemos clasificado estas pruebas en dos niveles diferentes:

2. 1. Pruebas de seguridad básicas

Es posible hacer algunas pruebas de seguridad básicas que reflejan fortalezas y debilidades en diferentes niveles del software utilizado. En esta prueba se buscan debilidades conocidas en el computador que entregue la Registraduría para realizar las pruebas. Se identifican posibles riesgos generados por la configuración del equipo.

2.2. Auditoría de seguridad web y documental

Se habla en este documento de una auditoría de seguridad web y documental cuando se hace una evaluación más profunda del sistema que no se limita solamente al equipo entregado por la Registraduría sino sobre la totalidad del sistema. Se evalúa la confidencialidad, integridad y disponibilidad de la información, la seguridad de la plataforma web y la seguridad de la infraestructura que lo componen.

3. Auditoría al software (funcionales, no funcionales y de estrés)

La auditoría del software busca evaluar la operación de una aplicación o programa específico. Evaluar que haga lo que debe hacer, conocer como lo hace y establecer sus límites.

La aplicación de la auditoría en una escala progresiva de estos tres elementos (incluyendo en segundo en su versión más básica o más compleja) es lo que nos permite la construcción de los tres escenarios descritos a continuación.

Considerando esto tipos de auditoria, presentamos a continuación tres escenarios posibles para auditar el sistema de escrutinio de las elecciones de 2018 en Colombia.

5.1 Escenario 1. Auditoría documental y pruebas de seguridad básicas

5.1.1 Actividades escenario 1

- Auditoría documental y de calidad basadas en la norma ISO9001.

- Revisión requerimientos contractuales vs entregables.
- Revisión del sistema de calidad empleado por el contratista para el desarrollo de las actividades contractuales.
- Programa auditoria.
- Plan de auditoría.
- Listas de chequeo.
- Mapas de riesgos.
- Informe de auditoría.

- Pruebas de seguridad básicas

- Revisión de equipos utilizados en el proceso de escrutinio en búsqueda de debilidades comunes.
- Canales de comunicaciones.
- Usuarios locales.
- Endurecimiento del sistema.
- Accesos de red.
- Configuración hardware inalámbrico.
- Software instalado.
- Escalamiento de privilegios.
- Modificación del entorno.

5.1.2 Presupuesto escenario 1

Considerando la complejidad del sistema tan solo a través de lo que podemos aprender del mismo en el contrato y en lo discutido con la MOE, se ha planteado un equipo, con un tiempo estimado de dedicación y se han calculado tarifas de servicios promedio en el mercado actual colombiano.

Auditoría documental - Calidad					
Cargo	**#**	**Horas x Semana**	**Semanas**	**$Hora**	**$Total**
Gerente	1	8	16	$180,000.00	$23,040,000.00
Auditor Líder 9001-MECI	1	40	16	$150,000.00	$96,000,000.00
Auditor	2	40	16	$100,000.00	$128,000,000.00
Documentador	1	40	16	$40,000.00	$25,600,000.00
Total					**$272,640,000.00**

Auditoria básica seguridad					
Cargo	**#**	**Horas x Semana**	**Semanas**	**$Hora**	**$Total**
Ingeniero CEH Líder	1	40	4	$200,000.00	$32,000,000.00
Ingeniero CEH	1	40	4	$140,000.00	$22,400,000.00
Total					**$54,400,000.00**

5.2 Escenario 2. Auditoría documental, pruebas de seguridad básicas y pruebas de software

5.2.1 Actividades escenario 2

- Auditoría documental y de calidad basadas en la norma ISO9001.

- Revisión requerimientos contractuales vs entregables.
- Revisión del sistema de calidad empleado por el contratista para el desarrollo de las actividades contractuales.
  - -Programa auditoria.
  - -Plan de auditoría.
  - -Listas de chequeo.
  - -Mapas de riesgos.
  - -Informe de auditoría.

- Pruebas de seguridad básicas.

-Revisión de equipos utilizados en el proceso de escrutinio en búsqueda de debilidades comunes.
  - Canales de comunicaciones.
  - Usuarios locales.
  - Endurecimiento del sistema.
  - Accesos de red.
  - Configuración hardware inalámbrico.
  - Software instalado.
  - Escalamiento de privilegios.
  - Modificación del entorno.

- Pruebas de software.
  - Pruebas funcionales.
  - Prueba no funcionales.
  - Pruebas de estrés.

5.2.2 Presupuesto escenario 2

Considerando la complejidad del sistema tan solo a través de lo que podemos aprender del mismo en el contrato y en lo discutido con la MOE, se ha planteado un equipo, con un tiempo estimado de dedicación y se han calculado tarifas de servicios promedio en el mercado actual colombiano.

Auditoría documental - Calidad					
Cargo	**#**	**Horas x Semana**	**Semanas**	**$Hora**	**$Total**
Gerente	1	8	16	$180,000.00	$23,040,000.00
Auditor Líder 9001-MECI	1	40	16	$150,000.00	$96,000,000.00
Auditor	2	40	16	$100,000.00	$128,000,000.00
Documentador	1	40	16	$40,000.00	$25,600,000.00
Total					**$272,640,000.00**

Auditoria básica seguridad					
Cargo	**#**	**Horas x Semana**	**Semanas**	**$Hora**	**$Total**
Ingeniero CEH Líder	1	40	4	$200,000.00	$32,000,000.00
Ingeniero CEH	1	40	4	$140,000.00	$22,400,000.00
Total					**$54,400,000.00**

Pruebas de software (funcionales, no funcionales y de estrés)					
Cargo	**#**	**Horas x Semana**	**Semanas**	**$Hora**	**$Total**
Gerente	1	8	8	$180,000.00	$11,520,000.00
Ingeniero QA Líder	1	40 8		$200,000.00	$64,000,000.00
Ingeniero QA	3	40 8		$100,000.00	$96,000,000.00
Total					**$171,520,000.00**

5.3 *Escenario 3. Auditoría documental, pruebas de seguridad básicas, pruebas de software y pruebas de seguridad web*

5.3.1 *Actividades escenario 3*

- Auditoría documental y de calidad basadas en la norma ISO9001.

-Revisión requerimientos contractuales vs entregables.
-Revisión del sistema de calidad empleado por el contratista para el desarrollo de las actividades contractuales.

- Programa auditoria.
- Plan de auditoría.
- Listas de chequeo.
- Mapas de riesgos.
- Informe de auditoría.

- Pruebas de seguridad básicas.

- Revisión de equipos utilizados en el proceso de escrutinio en búsqueda de debilidades comunes.
- Canales de comunicaciones
- Usuarios locales
- Endurecimiento del sistema
- Accesos de red
- Configuración hardware inalámbrico
- Software instalado
- Escalamiento de privilegios
- Modificación del entorno

- Pruebas de software
  - Pruebas funcionales
  - Prueba no funcionales
  - Pruebas de estrés

- Auditoría de seguridad web y documental

- Revisión GAP 27001.
  - Revisión prácticas, procedimientos y documentación de seguridad frente a la norma ISO27001.
  - Informe GAP.
  - Análisis de riesgos.
- Pruebas basadas en el proyecto top 10 de OWASP.
  - A1 Injection.
  - A2 Broken Authentication and Session Management.
  - A3 Cross-Site Scripting (XSS).
  - A4 Insecure Direct Object References.
  - A5 Security Misconfiguration.
  - A6 Sensitive Data Exposure.
  - A7 Missing Function Level Access Control.
  - A8 Cross-Site Request Forgery (CSRF).
  - A9 Using Components with Known Vulnerabilities.
  - A10 Unvalidated Redirects and Forwards.

5.3.2 *Presupuesto escenario 3*

Auditoría documental - Calidad					
Cargo	**#**	**Horas x Semana**	**Semanas**	**$Hora**	**$Total**
Gerente	1	8	16	$180,000.00	$23,040,000.00
Auditor Líder 9001-MECI	1	40	16	$150,000.00	$96,000,000.00
Auditor	2	40	16	$100,000.00	$128,000,000.00
Documentador	1	40	16	$40,000.00	$25,600,000.00
Total					**$272,640,000.00**

Auditoria básica seguridad					
Cargo	**#**	**Horas x Semana**	**Semanas**	**$Hora**	**$Total**
Ingeniero CEH Líder	1	40 4		$200,000.00	$32,000,000.00
Ingeniero CEH	1	40 4		$140,000.00	$22,400,000.00
Total					**$54,400,000.00**

Pruebas de software (funcionales, no funcionales y de estrés)					
Cargo	**#**	**Horas x Semana**	**Semanas**	**$Hora**	**$Total**
Gerente	1	8	8	$180,000.00	$11,520,000.00
Ingeniero QA Líder	1	40	8	$200,000.00	$64,000,000.00
Ingeniero QA	3	40	8	$100,000.00	$96,000,000.00
Total					**$171,520,000.00**

Auditoría de seguridad web y documental					
Cargo		**Horas x Semana**	**Semanas**	**$Hora**	**$Total**
Gerente	1	8	16	$180,000.00	$23,040,000.00
Auditor Lider Seguridad 27001	1	40	16	$150,000.00	$96,000,000.00
Auditor Líder Continuidad 22301	1	40	8	$200,000.00	$64,000,000.00
Ingeniero CEH Líder	2	40	16	$200,000.00	$256,000,000.00
Ingeniero CEH	1	40	16	$140,000.00	$89,600,000.00
Documentador	1	40	16	$40,000.00	$25,600,000.00
Total					**$554,240,000.00**

6 Opciones de auditoría para las elecciones de 2018

Opciones de auditoría para las elecciones de 2018

El ejercicio de plantear los escenarios posibles nos indica que el ideal de auditoría para 2018 corresponde a los siguientes módulos/valores:

	Módulos	**Plazo**	**# Personas**	**Valor**
Escenario 1	*Auditoría Documental - calidad*	16 semanas	5	$272.640.000,oo
	Pruebas de seguridad básicas	4 semanas	2	$54.400.000.oo
	TOTAL ESCENARIO 1	**16 semanas**	**7**	**$327.040.000,oo**
Escenario 2	*Auditoría Documental - calidad*	16 semanas	5	$272.640.000,oo
	Pruebas de seguridad básicas	4 semanas	2	$54.400.000.oo
	Pruebas de software (funcionales, no funcionales y de estrés)	8 semanas	5	$171.520.000,oo
	TOTAL ESCENARIO 2	**16 semanas**	**13**	**$498.560.000,oo**

Escenario 3	*Auditoría Documental - calidad*	16 semanas	5	$272.640.000,oo
	Pruebas de seguridad básicas	4 semanas	2	$54.400.000.oo
	Pruebas de software (funcionales, no funcionales y de estrés)	8 semanas	5	$171.520.000,oo
	Auditoría de seguridad Web y Documental	16 semanas	7	$554.240.000,oo
	TOTAL ESCENARIO 3	**16 semanas**	**13**	**$1.052.800.000,oo**

De acuerdo con este cuadro una auditoría básica costaría aproximadamente $327.000.000 requeriría de un equipo de 7 personas y duraría 4 meses. Mientras que nuestro escenario ideal puede ser inalcanzable pues el valor supera los $1.000.000.000, requiere de un equipo de 13 personas y si todos trabajan coordinadamente el plazo será de 4 meses.

Creemos que el panorama que presenta este documento es razonable si consideramos que en Colombia en 2014 la Registraduría Nacional del Estado Civil realizó un **"ESTUDIO DE NECESIDAD PARA CONTRATAR UN SISTEMA DE AUDITORÍA EXTERNA AL PROCESO ELECTORAL PARA LAS ELECCIONES DE CONGRESO, PARLAMENTO ANDINO Y PRESIDENTE Y VICEPRESIDENTE PRIMERA VUELTA, A REALIZARSE EN EL AÑO 2014".**

La evaluación buscaba establecer los requerimientos para una auditoría externa para "realizar un examen crítico sistemático y objetivo, además certificar el cumplimiento de manera integral, transparente y eficaz de los contratos números 243, 246, 248, 251, 253 de 2013, los cuales corresponden a los componentes de los procesos para preconteo, plan de comunicación y seguridad informática, digitalización de las actas de escrutinio E-14, escrutinio, información a votantes y call center, consolidación y divulgación nacional de resultados electorales, jurados de votación, censo electoral, inscripción y sorteo de candidatos, kit Electoral y biometría para las elecciones de Congreso, Parlamento Andino y Presidente y Vicepresidente primera vuelta, a realizarse el 9 de marzo y 25 de mayo de 2014, respectivamente". El resultado planteó las siguientes necesidades; un plazo de 6 meses, un presupuesto de $4.999.306.200 incluido IVA y un equipo de 73 personas con la siguiente composición:

Un (1) Gerente de proyecto
Un (1) Coordinador técnico
Dos (2) Especialistas en Seguridad y Auditoría de Sistemas de Información
Un (1) Coordinador jurídico
Dos (2) abogados especialistas en Contratación Estatal
Un (1) Asesor,
Un (1) profesional en derecho
Un equipo de treinta y cuatro (34) profesionales en Ingeniería Industrial, de Sistemas, Electrónica, telemática
Un equipo de veintiocho (28) profesionales
Dos (2) contadores públicos

Por su parte, en México la auditoría de software que se realizó del 21 de marzo al 1 de junio de 2017 (2 meses y medio) la realizó el laboratorio de cómputo del centro tecnológico de Aragón, entidad dependiente de la Universidad Nacional Autónoma de México, a cargo de 6 profesionales. Sin embargo, no conocemos el valor.

Los ejemplos no coinciden con el alcance de lo propuesto en este documento pero nos muestran que nuestros presupuestos en tiempo, equipo y valor no están muy lejos de la realidad.

Ahora bien, dado que los recursos con que contamos son limitados seguramente tendremos que hacer ajustes a los escenarios para cumplir con los requerimientos de tiempo y valor.

Por lo anterior, proponemos lo siguiente:

1. Priorizar. En cada módulo considerando recursos económicos y de personal se puede priorizar las actividades a realizar.

El ejemplo más concreto de esto es el del módulo documental. Al pedir los documentos y al recibirlos se pueden clasificar los que corresponda a escrutinio o desechar los que no se refieran a escrutinio (según corresponda). Es posible que este ejercicio disminuya sustancialmente la cantidad de documentos pertinentes para auditar. Sin embargo, esto solo se sabrá a la hora de recibir estos documentos.

2. Utilizar metodología de muestreo. Según los recursos económicos y de personal con que se cuente se puede hacer un muestreo y tan solo analizar lo que se ha priorizado o incluso una parte de cada una de las prioridades.

3. Realizar las labores con voluntarios. Se puede abrir una convocatoria y solicitar apoyo de voluntarios especializados para este proceso. El problema de esto es que el tiempo es corto y muy probablemente los voluntarios tengan poco tiempo para dedicar. Si se va a descargar la labor en voluntarios se necesitará en todo caso un coordinador que pueda distribuir, organizar y luego integrar ese trabajo.

Cada una de las decisiones que se tomen para ajustar los escenarios a recursos más limitados va a significar una disminución en la calidad de los resultados que se buscan. Pero, en todo caso, el ejercicio que resulte no será despreciable si se considera que se trata del primero de este tipo.

Bibliografía

Bibliografía

Aparicio, Javier. "Análisis Estadístico De La Elección Presidencial De 2006 ¿Fraude O Errores Aleatorios?". Política Y Gobierno, 2009, 225-243.

Bjørstad, Tor, and Mnemonic. Technical Report Source Code Audit Of Norwegian Electronic Voting System. Oslo: Mnemonic, 2013.

Bundesverfassungsgericht. Use Of Voting Computers In 2005 Bundestag Election Unconstitutional. Berlin, 2009.

Busaniche, Beatriz. Voto Electrónico Una Solución En Busca De Problemas. Buenos Aires: Fundación Vía Libre & Heinrich Böll, 2017.

CONICET. Análisis De Factibilidad En La Implementación De Tecnología En Diferentes Aspectos Y Etapas Del Proceso Electoral. Buenos Aires: CONICET, 2017.

Council of Europe (CoE). Certification of e-voting systems Guidelines for developing processes that confirm compliance with prescribed requirements and standards. Strasbourg: CoE, 2011.

Council of Europe (CoE). LEGAL, OPERATIONAL AND TECHNICAL STANDARDS FOR E-VOTING. Strasbourg: CoE, 2004.

Crónica. "La UNAM Auditará El Programa De Resultados Electorales Preliminares Que Se Usará En Julio", 2018. http://www.cronica.com.mx/notas/2018/1059207.html.

Defensoría del Pueblo de la C.A.B.A. DVT 56-504: Auditoría De Sistema De Votación Electrónica 2015 Para La Defensoría Del Pueblo De La C.A.B.A.. Buenos Aires: CABA, 2015.

Election Assistance Commission. Voluntary Voting System Guidelines. Washington: EAC, 2005.

Election Assistance Commission. Voting System Testing and Certification Program. Washington: EAC, 2011.

El Disenso. "Opacidad Electoral: Le Pagaron A Un Empleado Del Ministerio Del Interior Para Que Audite El Escrutinio Provisorio Desde Su ONG", 2017. http://www.eldisenso.com/politica/opacidad-electoral-frigerio-le-pago-empleado-suyo-audite-escrutinio-provisorio-indra-desde-una-ong/.

El Grillo. "Conozca Los Escándalos De Indra, La Empresa Encargada Del Conteo Electrónico En Las Próximas Elecciones", 2016. http://elgrillo.do/2016/05/conozca-los-escandalos-indra-la-empresa-cargo-del-conteo-electronico-las-proximas-elecciones/.

El Día. "El Kirchnerismo Siembra Sospechas Sobre El Escrutinio Elec-

toral", 2017. http://www.eldia.com/nota/2017-10-10-2-29-54-el-kirchnerismo-siembra-sospechas-sobre-el-escrutinio-electoral-la-provincia.

Iprofesional. "Advierten Que La Etapa Informática Del Escrutinio De Las Elecciones Del Domingo Es "Una Gran Caja Negra"", 2017. http://www.iprofesional.com/notas/257449-software-provincia-de-buenos-aires-gobierno-elecciones-kirchnerismo-computadora-correo-argentino-Advierten-que-la-etapa-informatica-del-escrutinio-de-las-elecciones-del-domingo-es-una-gran-caja-negra?page_y=0.

Infobae. "Piden Auditar El Escrutinio Provisorio Que Realizarán El Correo Argentino Y La Empresa INDRA", 2017. https://www.infobae.com/politica/2017/07/05/piden-auditar-el-escrutinio-provisorio-que-realizaran-el-correo-argentino-y-la-empresa-indra/.

Institutt for samfunnsforskning. Internet Elections- What Do The Voters Think?. Oslo: Institutt for samfunnsforskning, 2014.

International Federation for Electoral Systems (IFES). Electronic Voting & Counting Technologies A Guide to Conducting Feasibility Studies. Edited by Ben Goldsmith. Washington: IFES, 2011.

International Institute for Democracy and Electoral Assistance (IDEA). Certification of ICTs in Elections. Stockholm: IDEA, 2015.

International Institute for Democracy and Electoral Assistance (IDEA). International Electoral Standards Guidelines for reviewing the legal framework of elections. Stockholm: IDEA, 2002.

International Institute for Democracy and Electoral Assistance (IDEA). Introducing Electronic Voting: Essential Considerations. Stockholm: IDEA, 2011.

Kommunal og Regional Departementet. Electronic Voting: Challenges And Opportunities. Oslo, 2006. Disponible en: https://www.regjeringen.no/no/dokumenter/elektronisk-stemmegivning---utfordringer/id278479/

La Politica Online. "Confirmado: El Gobierno Le Dio A Indra El Control Del Escrutinio Provisorio", 2017. http://www.lapoliticaonline.com/nota/106363/.

La Nación. "Filtran El Software De Control De Una Máquina De Voto Electrónico Usada En Salta", 2017. http://www.lanacion.com.ar/2054577-filtran-el-codigo-de-una-maquina-de-voto-electronico-de-salta-y-alertan-sobre-los-riesgos-del-sistema.

La Nación. "Filtran Parte Del Código Fuente De La Boleta Electrónica Porteña", 2015. http://www.lanacion.com.ar/1803251-filtran-parte-del-codigo-fuente-de-la-boleta-electronica-portena.

Massey, Andrew. "But We Have to Protect Our Source: How Electronic Voting Companies' Proprietary Code Ruins Elections." Hastings Comm. & Ent. LJ 27, 2004.

McGaley, Margaret, and Joe McCarthy. "Transparency and E-Voting: Democratic Vs. Commercial Interests." Electronic Voting in Europe 47, 2004:

Misión de Observación Electoral. Implementación Del Voto Electrónico En Colombia. Bogotá: MOE, 2014.

National Democratic Institute for International Affairs, and International

Foundation for Electoral Systems. Implementing and Overseeing Electronic Voting and Counting Technologies. Washington: IFES & NDI, 2013.

Nederlandse Grondwet. Evaluatie Van De Tweede Kamerverkiezing, 2017. Disponible en: https://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vkf8vkdibryu

Organización de los Estados Americanos (OEA). Informe final de la misión de observación electoral de la organización de los estados americanos sobre el proceso electoral federal 2011- 2012. OEA, 2012.

Organización de los Estados Americanos (OEA). Tecnologías Aplicadas Al Ciclo Electoral. OEA, 2014.

OSCE Office for Democratic Institutions and Human Rights (ODIHR). Election Observation Handbook. Warsaw: OSCE, 2010.

OSCE Office for Democratic Institutions and Human Rights (ODIHR). Handbook For the Observation of New Voting Technologies. Warsaw: OSCE, 2013.

OSCE/ODIHR. NORWAY PARLIAMENTARY ELECTIONS 9 SEPTEMBER 2013. Warsaw: OSCE, 2013.

Teknisk Ukeblad. "Error In Encryption Of Email Voices", 5 de septiembre de 2013. https://www.tu.no/artikler/feil-i-krypteringen-av-e-stemmer/234436

The Carter Center. Developing a Methodology for Observing Electronic Voting. Atlanta: The Carter Center, 2007.

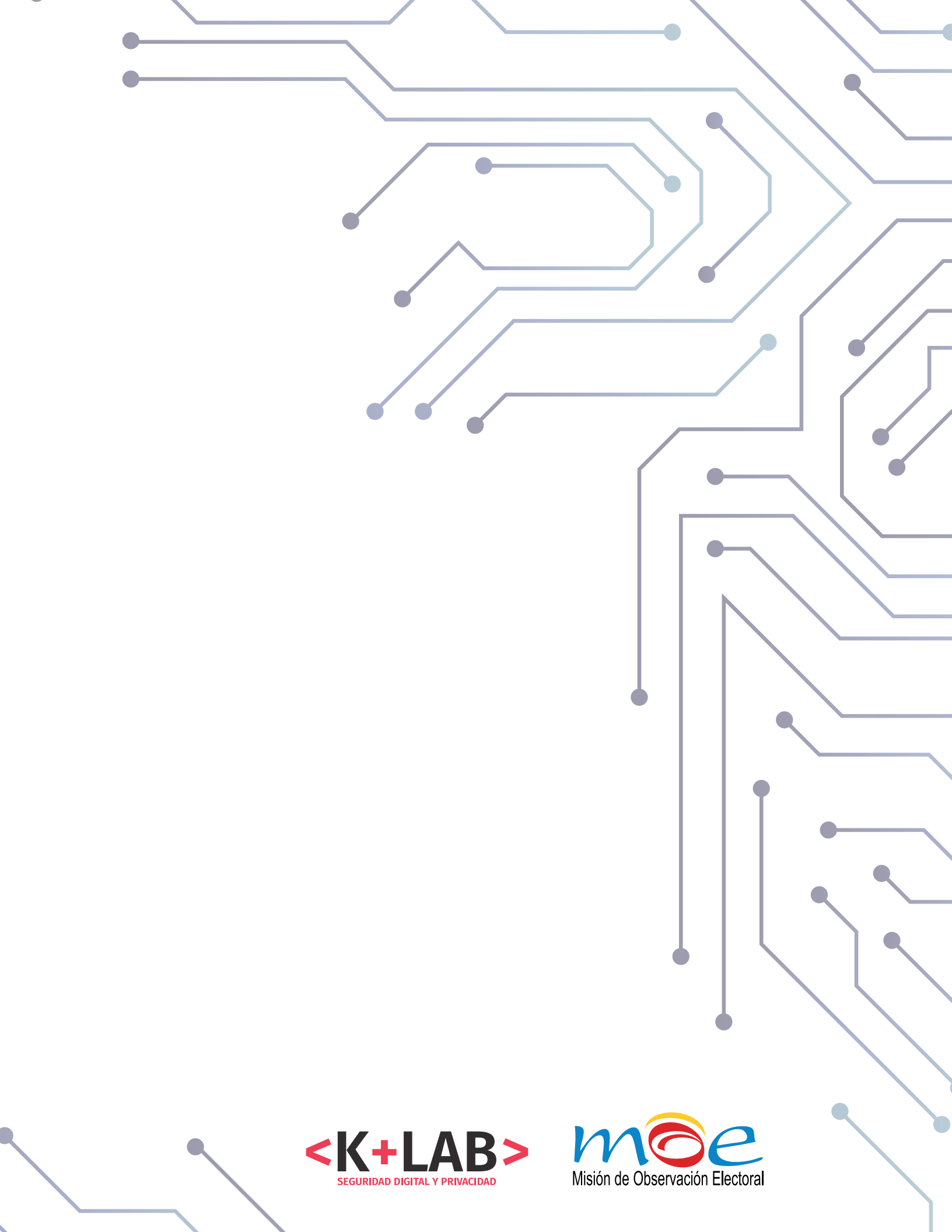
The Carter Center. The Carter Center Handbook on Observing Electronic Voting. Atlanta: The Carter Center, 2012.

The Carter Center. Internet Voting Pilot: Norway'S 2013 Parliamentary Elections. Washington: The Carter Center, 2014.

The Guardian. "German Hackers Find Security Hole In Software Used For Vote Counts", 2017. https://www.theguardian.com/world/2017/sep/08/german-hackers-find-security-hole-in-software-used-for-vote-counts.

United Nations Development Program (UNDP). Electoral Results Management Systems: Catalogue of Options A guide to support electoral administrators and practitioners to evaluate RMS options, benefits and challenges. UNDP, 2015.

Volkamer, Melanie. "Electronic Voting in Germany." In Data Protection in a Profiled World, 177-89: Springer, 2010.


<K+LAB>
SEGURIDAD DIGITAL Y PRIVACIDAD
moe
Misión de Observación Electoral