IIDH / CAPEL

INSTITUTO INTERAMERICANO DE DERECHOS HUMANOS
CENTRO DE ASESORÍA Y PROMOCIÓN ELECTORAL

AUDITORÍA DE SISTEMAS

AUDITORÍA EXTERNA INTERNACIONAL

Elecciones al Congreso y Consultas Populares 2026,
Registraduría Nacional del Estado Civil, Colombia

INFORME DE CIERRE
DICTAMEN FINAL
DE AUDITORÍA

INFORME POST ELECTORAL

CONTENIDO

I. INTRODUCCIÓN

El presente documento constituye el Informe de cierre post electoral y dictamen Final de Auditoría de Sistemas correspondiente al proceso electoral de Elecciones al Congreso de la República y Consultas Populares 2026. Se elabora en el marco del Convenio de Cooperación Internacional No. 098, suscrito entre la Registraduría Nacional del Estado Civil y el Instituto Interamericano de Derechos Humanos (IIDH), a través del Centro de Asesoría y Promoción Electoral (CAPEL).

Este dictamen final integra y consolida los resultados de todos los informes técnicos emitidos durante el ciclo de auditoría, así como los resultados evidenciados en etapa post-electoral.

II. ANTECEDENTES

Contexto normativo, técnico y operativo

En el marco del fortalecimiento institucional de los procesos electorales colombianos, la Registraduría Nacional del Estado Civil (RNEC) suscribió el Convenio de Cooperación Internacional No. 098 con el Instituto Interamericano de Derechos Humanos (IIDH).

El contexto en que se desarrolla esta auditoría se caracteriza por la complejidad de los activos tecnológicos involucrados. Los sistemas electorales operan bajo condiciones de alta demanda simultánea, tiempos de operación comprimidos y una exigencia extrema sobre la disponibilidad, integridad y confidencialidad de la información. Cualquier falla en estos atributos —reconocidos en los principios de la norma ISO/IEC 27001 como pilares de la seguridad de la información— tendría un impacto directo sobre la confianza ciudadana en el resultado electoral.

Asimismo, el proceso electoral 2026 se materializó mediante contratos de prestación de servicios tecnológicos de alta especialización (contratos 049 y 060 de 2025), cuya correcta ejecución debía ser verificada por una entidad auditora externa, independiente y con estándares internacionales. En este contexto, la Auditoría de Sistemas tiene una doble función: por un

lado, verificar el cumplimiento técnico frente a los criterios contractuales; por otro, identificar riesgos tecnológicos que pudieran comprometer la integridad del proceso.

Insumos que anteceden este informe de cierre

Durante los procesos de trabajo de campo se entregó la siguiente cadena documental, generada de forma progresiva durante la ejecución de la auditoría.

- Informe Preliminar de Auditoría de Sistemas (24 de febrero de 2026).
- Resumen Ejecutivo del Informe Preliminar (24 de febrero de 2026)
- Informe de Seguimiento de Hallazgos (6 de marzo de 2026).
- Informe del Día Electoral — Seguridad e Infraestructura (8 de marzo de 2026).
- Informe estado de situación (9 de abril de 2026).

Los informes presentados con anterioridad permiten construir una visión longitudinal del ecosistema tecnológico electoral: desde el alistamiento de los sistemas en la etapa pre-electoral, pasando por su operación bajo condiciones reales de alta demanda el día de las elecciones, hasta la validación en la atención de los hallazgos de cada componente en la etapa post-electoral.

III. DESCRIPCIÓN GENERAL DE LA AUDITORÍA

A continuación, se detalla el marco estructural y metodológico que rigió la ejecución de la presente evaluación. Este apartado desglosa los objetivos generales y específicos trazados, así como la delimitación precisa de los alcances general y tecnológico de la auditoría. Asimismo, se expone la metodología de evaluación implementada a través de sus cuatro fases secuenciales: planificación, trabajo de campo, informes y recomendaciones, y seguimiento. Dentro del desarrollo del trabajo de campo, se especifican las dimensiones de la evaluación abordadas, y finalmente, se establece el sistema formal para la categorización de los resultados obtenidos y los criterios de auditoría aplicados, que garantizaron un análisis objetivo, sistemático y alineado con los estándares internacionales en la materia.

3.1 Objetivos de la auditoría

3.1.1 Objetivo general

Realizar una evaluación integral de los sistemas de información correspondientes a jurados de votación, preconteo, escrutinio y consolidación y divulgación nacional, así como de la infraestructura tecnológica y los recursos informáticos implementados para las elecciones de 2026, con el fin de fortalecer la transparencia, integridad, confiabilidad y credibilidad del proceso electoral.

3.1.2 Objetivos específicos

1. Auditar los sistemas electorales a través de una revisión del código fuente, evaluación de su funcionalidad y la verificación de la integridad y consistencia de los datos procesados.

2. Verificar la seguridad de la información, mediante la ejecución de pruebas de penetración, el análisis de vulnerabilidades y la evaluación de los mecanismos de control de accesos y gestión de usuarios.

3. Evaluar los procesos asociados a los sistemas electorales, asegurando la trazabilidad de los datos y la correcta validación de los flujos de información entre los diferentes componentes del proceso electoral.

4. Auditar la infraestructura tecnológica, con el fin de verificar su disponibilidad, capacidad de redundancia y mecanismos de continuidad del servicio durante las distintas etapas del proceso electoral.

5. Documentar los hallazgos técnicos y operativos, elaborando informes detallados que evidencien las debilidades u observaciones, riesgos identificados y oportunidades de mejora en cada uno de los sistemas auditados.

6. Formular recomendaciones técnicas y procedimentales, orientadas al fortalecimiento de la seguridad, eficiencia y confiabilidad de los sistemas de información y procesos electorales.

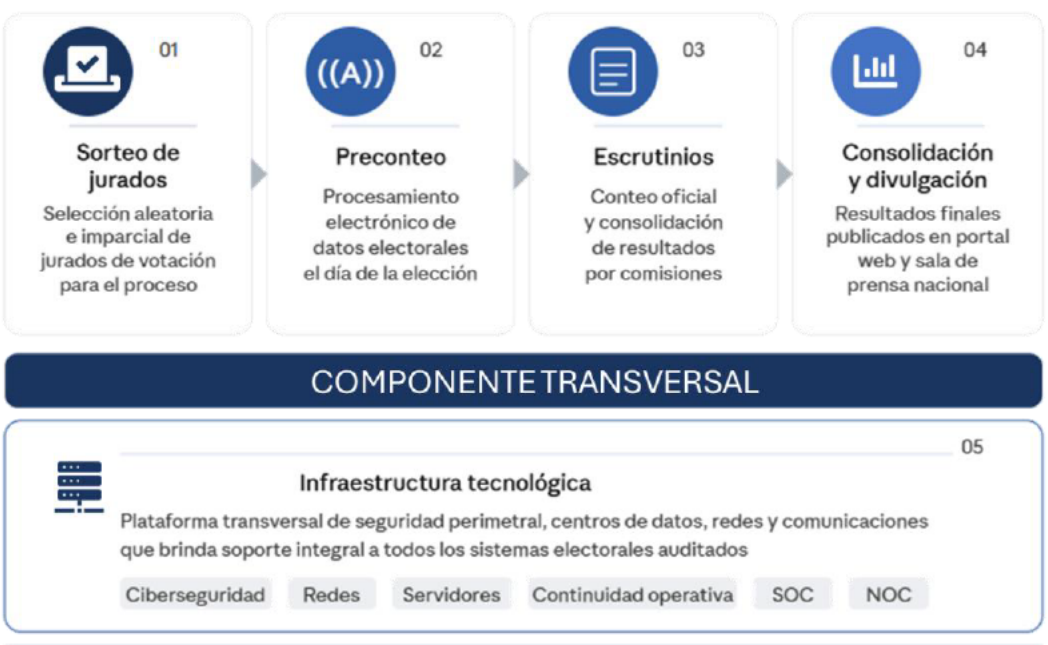
7. Realizar seguimiento a las acciones correctivas, validando la implementación de las correcciones y mejoras adoptadas en los sistemas y procesos auditados.

3.2 Alcance de la auditoría

Se estableció la ejecución de una auditoría técnica integral, independiente y con rigor internacional sobre los sistemas de información, la infraestructura tecnológica y los procesos asociados a la organización, ejecución y cierre de las jornadas electorales correspondientes al periodo 2026. La evaluación comprendió un seguimiento sistemático y progresivo a través de las etapas pre-electoral, electoral y post-electoral, con el objetivo de verificar el diseño, desarrollo, configuración, implementación y control de los sistemas, así como los procedimientos operativos subyacentes.

Asimismo, se integró el análisis de riesgos técnicos, logísticos y de cumplimiento alineados con estándares internacionales, la validación de la efectividad de los controles implementados, el seguimiento a la subsanación de observaciones previos y la emisión de los informes técnicos pertinentes para robustecer la transparencia, integridad y confianza institucional en los procesos gestionados por la Registraduría Nacional del Estado Civil.

La delimitación técnica abarcó la revisión detallada de los componentes de software de misión crítica, específicamente los sistemas de gestión de jurados de votación, preconteo, escrutinio, consolidación y divulgación nacional de resultados. A nivel de infraestructura, la auditoría evaluó los recursos informáticos, plataformas tecnológicas, redes de comunicación, centros de datos y mecanismos de transmisión de datos operativos. A nivel de seguridad se concentró en verificar que el conjunto de componentes tecnológicos involucrados en los sistemas cuenta con los controles necesarios para garantizar la integridad, disponibilidad y confidencialidad de la información. A nivel de software se concentró en la revisión detallada del diseño, documentación técnica, documentación de usuario, casos de uso, casos de prueba, sistemas operativos, entre otros y a nivel de procesos se enfocó en las métodos y procedimientos para el uso de los sistemas, incluyendo actividades integrales clave para el éxito del proceso como la capacitación y soporte técnico.



3.3 Metodología de evaluación

El proceso de auditoría de sistemas se ejecutó mediante un enfoque estructurado en cuatro fases sucesivas: la planificación, orientada a definir la estrategia e identificar los cinco sistemas críticos de la operación; el trabajo de campo, que abarcó evaluaciones técnicas especializadas en software, seguridad de la información, trazabilidad de procesos e infraestructura tecnológica; la fase de informes y recomendaciones, centrada en la documentación técnica de los hallazgos; y el seguimiento, destinado a validar las correcciones aplicadas y revisión de mejoras implementadas en sistemas y procesos.

3.3.1 Dimensiones de evaluación para el trabajo de campo

Para cada componente, la auditoría se estructuró en cuatro dimensiones de análisis técnico en el trabajo de campo:

- Auditoría de Software: revisión del código fuente, funcionalidad, consistencia, documentación. Evaluación de los sistemas con el objetivo de verificar:
  - Que los procedimientos de diseño, desarrollo y versionado son adecuados.
  - Que cada sistema garantiza la funcionalidad correcta para la que fue contratado.
  - Que los aplicativos desarrollados se encuentren individualizados e identificados en un catálogo que permite validar su integridad.
  - Que las capacidades de parametrización se adecúan a los requerimientos.
  - Que se realiza una adecuada gestión y control de cambios.
  - Procesos de control de calidad y pruebas.
  - Que los casos de uso estén completos, detallados y acordes a las necesidades del proceso.
  - Casos de prueba exhaustivos y acordes a los casos de uso.
  - Análisis de los sistemas desde una perspectiva de desarrollo de software, de forma que sea posible identificar y determinar posibles funcionalidades defectuosas.
  - Integridad y consistencia de los datos y de la información transmitida.

- Que se garantiza la integridad de la información durante el procesamiento de datos.
- Que tiene controles y medidas de seguridad implementadas que permiten detectar un intento de vulneración de la información contenida.
- Revisión de código fuente.

- Auditoría de Seguridad: pruebas de penetración, análisis de vulnerabilidades, gestión de accesos. Actividades establecidas:
  - Verificación de los controles para arranque seguro de los servidores (data center) y equipos desplegados para usuario final.
  - Controles y niveles de aseguramiento sistemas operativos.
  - Controles de integridad que garantizan la inalterabilidad de datos electorales procesados en los diferentes sistemas.
  - Controles para garantizar la disponibilidad de los sistemas.
  - Análisis de vulnerabilidades.
  - Análisis de penetración utilizando como referencia OWASP Desktop App Security, entre otras.
  - Análisis de código fuente mediante ejecución de pruebas de código estático y dinámico.
  - Pruebas de caja gris.

- Auditoría de Procesos: trazabilidad de datos, validación de flujos de información. Revisión de:
  - El alcance y amplitud de manuales de sistemas;
  - Documentación de características funcionales y no funcionales de los sistemas;
  - Los procedimientos para la carga de los datos de la elección;
  - Los procedimientos para la aceptación de la versión de software que se pondrá en producción;
  - Los procedimientos para la verificación de la autenticidad del software a utilizar;
  - Procedimiento de despliegue y repliegue de los equipos (Aplica para escrutinio);
  - Procedimientos de almacenamiento, distribución y custodia de los equipos;
  - Procedimientos de soporte técnico y mesa de ayuda;

- Los procedimientos y herramientas de capacitación del personal técnico de soporte en campo y remoto;
- Los procedimientos y herramientas de capacitación de los usuarios de los sistemas

- Auditoría de Infraestructura Tecnológica: disponibilidad, redundancia, continuidad del servicio. Actividades establecidas:
  - Verificación de cumplimiento con todas las especificaciones técnicas definidas en el anexo técnico.
  - Verificación y validación de la capacidad, funcionalidad y operatividad de la solución informática.
  - Validación de las herramientas y procedimientos implementados de seguridad informática y de la información.
  - Verificación de que se asegura la confidencialidad, disponibilidad, escalabilidad de la infraestructura tecnológica.

3.3.2 Categorización de resultados

A continuación, se presenta la clasificación metodológica utilizada para categorizar los resultados obtenidos, estructurada rigurosamente según su nivel de impacto y criticidad técnica en el entorno evaluado:

- Fortalezas: prácticas sobresalientes que deben mantenerse dentro del ciclo electoral.
- Observaciones: Hace referencia a una oportunidad de mejora o a una situación identificada que, si bien no constituye un incumplimiento directo de las obligaciones contractuales o normativas, podría representar un riesgo potencial en el futuro. En estos casos, no se exige necesariamente un plan correctivo inmediato, pero se recomienda su atención preventiva como parte de las buenas prácticas de gestión y mejora continua.
- Hallazgos: Corresponde a una desviación comprobada frente a un criterio de auditoría previamente establecido, sustentada mediante evidencia verificable. Implica la existencia de un incumplimiento o debilidad significativa, por lo que genera una No Conformidad y requiere la definición de un Plan de Acción Correctiva por parte del responsable correspondiente.

3.4 Criterios de auditoría aplicados

La evaluación se realizó frente a los siguientes grupos de criterios de referencia:

Criterio	Aplicación en el encargo
Estándares internacionales de auditoría y gestión de TI (COBIT, ITAF, ISO/IEC 19011, 27001, 27002, 27005, OWASP, NIST)	Marco de referencia para evaluación basada en buenas prácticas y marcos de referencia reconocidos internacionalmente para la gestión, control y auditoría de tecnologías de la información, orientados a garantizar la eficiencia, confiabilidad y seguridad de los sistemas.
Seguridad de la información	Revisión de controles orientados a asegurar la confidencialidad, integridad, disponibilidad y trazabilidad de la información electoral, incluyendo mecanismos de control de accesos, gestión de identidades, monitoreo de eventos, protección de datos y gestión de incidentes de seguridad.
Controles sobre el ciclo de vida de los sistemas	Revisión de los controles implementados en las fases de desarrollo, pruebas, implementación, cambios, mantenimiento y operación de los sistemas de información utilizados en el proceso electoral.
Continuidad operativa y recuperación ante desastres	Evaluación de la infraestructura tecnológica que soporta los sistemas electorales, incluyendo centros de datos, redes, comunicaciones, plataformas tecnológicas y mecanismos de continuidad del negocio y recuperación ante desastres.
Pruebas técnicas y validación de funcionamiento	Realización de pruebas funcionales, técnicas y de seguridad, así como revisión de código fuente que permitan verificar que los sistemas de jurados de votación, preconteo, escrutinio, consolidación y divulgación nacional, operen conforme a los requerimientos establecidos.
Disponibilidad y desempeño de los sistemas críticos	Verificación de que los sistemas tecnológicos cuenten con niveles adecuados de disponibilidad, capacidad, rendimiento y escalabilidad para soportar la demanda del proceso electoral.

IV. DESARROLLO DE LA AUDITORÍA EN LAS TRES ETAPAS

La auditoría se ejecutó bajo un enfoque basado en riesgos en cuatro fases metodológicas: planificación, trabajo de campo, elaboración de informes de hallazgos y seguimiento. Estas fases se articularon en las tres etapas del ciclo electoral: pre-electoral, jornada electoral y post-electoral.

4.1 Etapa Pre-Electoral

Durante la etapa pre-electoral, las actividades de planificación se orientaron a la revisión del alcance técnico, la identificación de los sistemas críticos y la coordinación de accesos. Se procedió a examinar documentación de diseño de software, diagramas de arquitectura, controles de seguridad, bases de datos y herramientas de gestión del ciclo de vida del desarrollo, así como a realizar entrevistas con el personal técnico responsable de cada componente.

El trabajo de campo incluyó la revisión del código fuente de los sistemas de Jurados de Votación, Preconteo (Regiones 1 y 2), Escrutinio, Consolidación y Divulgación; ejecución de análisis de código estático y dinámico; pruebas de penetración sobre componentes disponibles; validación de entornos de alta disponibilidad mediante revisión de la documentación de los centros de datos; y análisis de las políticas y procedimientos de seguridad de la información vigentes, análisis de documentación y procedimientos.

La gestión del desarrollo se verificó frente a estándares de la industria, constatándose la adopción de metodología ágil (Scrum), el uso de herramientas especializadas (Azure DevOps, Jira, GitHub), la implementación de pruebas automatizadas (Apache JMeter, Jenkins, SonarQube, PowerShell) y la existencia de procesos formales de control de calidad (QA).

4.2 Etapa Electoral — Jornada del 8 de marzo de 2026

Durante la jornada electoral, el trabajo se orientó a verificar si la infraestructura tecnológica y los mecanismos de protección perimetral respondieron adecuadamente a las condiciones reales de operación, en particular a la alta demanda de tráfico simultáneo generada por el acceso ciudadano y de medios al portal de resultados.

Se realizó la revisión de los registros operativos y métricas de infraestructura generados por la plataforma cloud (Amazon Web Services), los reportes de monitoreo continuo del Centro de Operaciones de Seguridad (SOC) y la supervisión del Centro de Operaciones de Red (NOC), así como el análisis de los logs del Firewall de Aplicaciones Web (AWS WAF). Asimismo, se analizó el comportamiento del tráfico generado por medios de comunicación nacionales e internacionales sobre el portal de resultados.

4.3 Etapa Post-Electoral

La etapa post-electoral comprendió la verificación técnica y documental del estado final de los sistemas, la evaluación completa de los componentes y la verificación formal del estado de las acciones correctivas adoptadas por en respuesta a los hallazgos documentados.

V. Resultados Relevantes

5.1 Fortalezas, Observaciones y Hallazgos

A continuación, se presentan los resultados de la evaluación a los sistemas y componentes tecnológicos. El contenido evidencia las fortalezas, observaciones y hallazgos identificados durante la revisión. Esta información fue detalladamente reportada en los informes de auditoría entregados previo a las elecciones del 8 e marzo.

Indicadores por componente			
Componente	Fortalezas	Observaciones	Hallazgos
Jurados de Votación	14	10	2
Preconteo	30	13	4
Escrutinio	11	8	4
Consolidación y Divulgación	11	10	1
Infraestructura tecnológica	5	3	1
TOTAL	71	44	12

5.1.1 Fortalezas

Esta sección presenta las 71 fortalezas identificadas durante la revisión de los cinco componentes incluidos en el alcance. Este consolidado agrupa 14 puntos en Jurados de Votación, 30 en Preconteo (divididos por regiones), 11 en Escrutinio, 11 en Consolidación y divulgación, y 5 en Infraestructura tecnológica, cuyos desgloses se exponen seguidamente:

5.1.1.1 Fortalezas en Jurados de Votación

Tras el análisis de las evidencias, se identificaron 14 fortalezas relacionadas principalmente al desempeño en el ciclo de vida del software, la gestión de datos y la continuidad del proceso electoral:

1. Procedimientos adecuados para la gestión del diseño y desarrollo de software.
2. Manejo adecuado del versionamiento del software.

3. El sistema garantiza la funcionalidad correcta para la que fue contratado.
4. Gestión individualizada e identificación de aplicativos en catálogo que permite validar su integridad.
5. Capacidades de parametrización adecuadas a los requerimientos.
6. Gestión y control de cambios adecuadamente implementados.
7. Procesos de control de calidad y pruebas implementados de manera estructurada.
8. Gestión efectiva de historias de usuario completas, detalladas y alineadas a las necesidades del proceso.
9. Casos de prueba exhaustivos y alineados con los requerimientos del proceso.
10. Análisis estructurado y modular del código fuente permite identificar y determinar posibles funcionalidades defectuosas.
11. Implementación de mecanismos técnicos y controles que aseguran la integridad y consistencia de los datos y la información transmitida.
12. Controles efectivos para garantizar la disponibilidad de los sistemas del proceso de Jurados.
13. Fortaleza en el Marco de Gobierno y Ciclo de Vida de Desarrollo de Software Seguro.
14. Suficiencia y claridad en el material de capacitación externa del sistema de Jurados de Votación.

5.1.1.2 Fortalezas en Preconteo

Para este componente se identificó un total de 30 fortalezas, distribuidas en 14 fortalezas para la Región 1 y 16 fortalezas para la Región 2. A continuación, se desglosan los hallazgos de cada zona:

Preconteo · Región 1 · 14 fortalezas

1. Adecuados procedimientos para la gestión del diseño, desarrollo y versionado del software.
2. Cumplimiento funcional integral del Sistema de Preconteo conforme a los requerimientos contractuales.
3. Individualización y gestión catalogada de los aplicativos que permite validar su integridad.

4. Capacidades de parametrización adecuadas y alineadas a los requerimientos contractuales.
5. Adecuada gestión y control de cambios en el ciclo de desarrollo del sistema.
6. Procesos estructurados de control de calidad y pruebas alineados con buenas prácticas de aseguramiento de la calidad.
7. Historias de usuario completas, detalladas y alineadas con las necesidades del proceso y los requerimientos contractuales.
8. Casos de prueba exhaustivos y coherentes con los casos de uso e historias de usuario.
9. Análisis técnico del software que permite identificar y determinar posibles funcionalidades defectuosas.
10. Mecanismos técnicos y controles efectivos que aseguran la integridad y consistencia de los datos e información transmitida.
11. Documentación técnica integral, estandarizada y clara para el proceso crítico de Preconteo. (Región 1 y Región 2).
12. Completa documentación sobre la metodología de desarrollo ágil, desarrollo de software seguro, plan de pruebas, gobierno de la arquitectura de software. (Región 1 y Región 2).
13. Modelo robusto de Gobernanza del Código Fuente, Seguridad en el Ciclo de Vida (DevSecOps) y Protocolo Formal de Custodia Legal del Software. (Región 1 y Región 2).
14. Fortaleza de Control: Programa integral de capacitación y transferencia de conocimiento para los perfiles operativos del sistema de Preconteo. (Región 1 y Región 2).

Preconteo · Región 2 · 16 fortalezas

1. Adecuados procedimientos para la gestión del diseño y desarrollo de software.
2. Manejo adecuado de versionamiento del software.
3. El sistema garantiza la funcionalidad correcta para la que fue contratado. (Región 1 y Región 2).
4. Individualización e identificación de aplicativos en un catálogo que permite validar su integridad.
5. Capacidades de parametrización adecuadas a los requerimientos.
6. Adecuada gestión y control de cambios.
7. Procesos de control de calidad y pruebas robustos y estructurados.

8. Historias de usuario completas, detalladas y acordes a las necesidades del proceso.
9. Casos de prueba exhaustivos y acordes a los casos de uso.
10. El análisis de los sistemas desde una perspectiva de desarrollo de software permite identificar y determinar posibles funcionalidades defectuosas.
11. Se implementaron mecanismos técnicos y controles adecuados para garantizar la integridad y consistencia de los datos y de la información transmitida.
12. Controles para garantizar la disponibilidad de los sistemas. (Región 1 y Región 2).
13. Documentación técnica integral, estandarizada y clara para el proceso crítico de Preconteo. (Región 1 y Región 2).
14. Completa documentación sobre la metodología de desarrollo ágil, desarrollo de software seguro, plan de pruebas, gobierno de la arquitectura de software. (Región 1 y Región 2).
15. Modelo robusto de Gobernanza del Código Fuente, Seguridad en el Ciclo de Vida (DevSecOps) y Protocolo Formal de Custodia Legal del Software. (Región 1 y Región 2).
16. Fortaleza de Control: Programa integral de capacitación y transferencia de conocimiento para los perfiles operativos del sistema de Preconteo. (Región 1 y Región 2).

5.1.1.3 Fortalezas en Escrutinio

El análisis integral aplicado al sistema de Escrutinio dio como resultado un consolidado de 11 fortalezas con el siguiente detalle:

1. Adecuados procedimientos para la gestión del diseño y desarrollo de software.
2. Manejo adecuado de versionamiento del software.
3. El sistema garantiza la funcionalidad correcta para la que fue contratado.
4. Los aplicativos desarrollados se encuentran individualizados e identificados en un catálogo que permite validar su integridad.
5. Capacidades de parametrización adecuadas a los requerimientos.
6. Gestión y control de cambios adecuado.

7. Procesos de control de calidad y pruebas estructurados y alineados con la metodología de aseguramiento de la calidad.
8. Las historias de usuario están completas, detalladas y acordes a las necesidades del proceso.
9. Casos de prueba exhaustivos y acordes a los casos de uso.
10. El análisis de los sistemas desde una perspectiva de desarrollo de software permite identificar y determinar posibles funcionalidades defectuosas.
11. No se encontraron hallazgos en la ejecución formal y documentada de análisis estático de código fuente mediante herramienta especializada.

5.1.1.4 Fortalezas en Consolidación y divulgación

La revisión técnica de este componente evidenció un total de 11 fortalezas, las cuales abarcan desde buenas prácticas de desarrollo hasta controles de infraestructura y seguridad:

1. Capacidades de parametrización adecuadas a los requerimientos.
2. Adecuada gestión y control de cambios.
3. Procesos de control de calidad y pruebas estructurado y en concordancia con la metodología de aseguramiento de la calidad de la empresa.
4. Casos de prueba exhaustivos y acordes a los casos de uso.
5. Código fuente estructurado alineado a buenas prácticas.
6. Suficientes medidas preventivas y reactivas ante incidentes.
7. Centros de Datos Redundantes (control Máximo dos DC).
8. Elementos de contingencia ante fallas.
9. Integración de logs al SOC de la RNEC.
10. Reporte inmediato de incidentes al SOC.
11. Se dispone de análisis de riesgos y controles declarados.

5.1.1.5 Fortalezas en Infraestructura tecnológica

La auditoría al componente de Infraestructura Tecnológica permitió identificar un total de 5 fortalezas relacionadas principalmente a la seguridad, robustez, documentación y soporte físico de la solución.

1. Diagramas documentales de los componentes de infraestructura de la solución.
2. Data Centers con robustas certificaciones de la industria.
3. Presencia de documentación detallada de las políticas y procedimientos de seguridad de la información para los sistemas auditados.
4. Matriz de Riesgo tecnológico de los procesos auditados.
5. Informes de Gestión de Operatividad y Ciberseguridad con énfasis en el monitoreo de eventos, alertas e incidentes.

5.1.2 Observaciones

Este apartado expone las 44 observaciones identificadas en la evaluación de los sistemas del proceso electoral. Conforme a la metodología establecida, estas situaciones hacen referencia a una oportunidad de mejora o a una situación identificada que, si bien no constituye un incumplimiento directo de las obligaciones contractuales o normativas, podría representar un riesgo potencial en el futuro; no se exige necesariamente un plan correctivo inmediato, pero se recomienda su atención preventiva como parte de las buenas prácticas de gestión y mejora continua.

La adecuada gestión las observaciones permitirá fortalecer los mecanismos de control, mejorar la operación de los sistemas evaluados y contribuir a la transparencia, confiabilidad y robustez tecnológica del proceso electoral.

El consolidado de observaciones abarca Jurados de votación (10), Preconteo (13), Escrutinio (8), Consolidación y divulgación (10) e Infraestructura tecnológica (3).

5.1.2.1 Observaciones en Jurados de votación

La revisión técnica de este componente dio como resultado un consolidado de 10 observaciones. Los puntos identificados se asocian principalmente a temas referentes a documentación del código, oportunidades de mejora en la gestión de capacitación del personal técnico y aspectos específicos de seguridad en la configuración de los aplicativos:

1. Fortalecimiento documental.
2. Continuidad operativa por documentación.
3. Documentación de procedimientos de aseguramiento (hardening) de sistemas operativos en el proceso de Jurados.
4. Ejecución de análisis de vulnerabilidades.
5. Entorno de pruebas para análisis de penetración.
6. Sanitización de Angular.
7. Configuración de trazas de ejecución y printStackTrace().
8. Marco formal de capacitación y repositorios estructurados de consulta para el personal de soporte técnico del sistema de Jurados de Votación.
9. Documentados de procedimientos sobre controles de integridad de los datos cargados automáticamente o mediante procesos por lotes.
10. Plan de Capacitación y Transferencia de Conocimiento del personal técnico.

5.1.2.2 Observaciones en Preconteo

El análisis del sistema de Preconteo registró un total de 13 observaciones centradas en la actualización de versiones de desarrollo, la gobernanza de herramientas de soporte y el aseguramiento del entorno de software:

1. Fortalecimiento documental.
2. Versiones de Java en el código fuente desarrollado.
3. Documentación de procedimientos de aseguramiento de sistemas operativos en el proceso de Preconteo (Región 1 y Región 2).
4. Ejecución de análisis de vulnerabilidades (Región 1 y Región 2).
5. Soporte y parcheo de versiones de Java en uso (Región 1).
6. Sustitución del análisis con depurador por capturas jstack (Región 1).

7. Documentación Operativa y Gobernanza en la Herramienta de Soporte TI. (Región 1).
8. ReCaptcha en autenticación.
9. Información y configuración de usuarios a través de servicios API.
10. Almacenamiento de tokens JWT.
11. Documentación de código fuente.
12. Versión de Java del código fuente desarrollado con soporte extendido.
13. Documentación Operativa y Gobernanza en la Herramienta de Soporte TI. (Región 2).

5.1.2.3 Observaciones en Escrutinio

Se identificaron 8 observaciones operativas y tecnológicas durante la evaluación del proceso de Escrutinio. Las observaciones listadas a continuación se enfocan en fortalecer la documentación técnica del código fuente, el soporte de las plataformas de desarrollo y la formalización de programas de capacitación continua:

1. Fortalecimiento documental.
2. Versión de Java en uso y su soporte oficial.
3. Documentación de procedimientos de aseguramiento (hardening) de sistemas operativos en el proceso de Escrutinio.
4. Ejecución de análisis de vulnerabilidades.
5. Entorno de pruebas para análisis de penetración.
6. Registro documental sobre normativas para la gestión de la configuración, versionado y aseguramiento del paso a producción.
7. Documentos sobre políticas y procedimientos para la seguridad y carga de información.
8. Programa de capacitación continua y Base de Conocimiento centralizada y su accesibilidad para los actores del proceso electoral.

5.1.2.4 Observaciones en Consolidación y divulgación

La auditoría al componente de Consolidación y divulgación evidenció un total de 10 observaciones. El siguiente desglose abarca aspectos de optimización en el código fuente, la estructuración de la documentación de requerimientos y la visibilidad de las capacidades y acuerdos de servicio de la solución integral:

1. Fortalecimiento documental.
2. Versiones de Java del código fuente desarrollado.
3. Evidencia documentada del proceso de levantamiento de requerimientos.
4. Consultas dinámicas en HQL
5. Parseo de XML (Interpretación de datos mediante componentes de software).
6. Documentación sobre el modelo integral de infraestructura tecnológica.
7. Disponibilidad documentada de la solución completa.
8. Capacidad del sistema completo.
9. Restauración del servicio.
10. Procedimientos de parchado y actualización.

5.1.2.5 Observaciones en Infraestructura tecnológica

La evaluación de la Infraestructura tecnológica permitió determinar 3 observaciones específicas de control. Estas observaciones preventivas se orientan a la optimización de las políticas de retención de logs, los mecanismos de integración de monitoreo y la alta disponibilidad de los sistemas:

1. Políticas de existencia y retención de logs a nivel de sistemas.
2. Integración de logs con herramientas de Monitoreo con el SIEM del RNEC.
3. Esquema de alta disponibilidad en modo Activo-Activo.

5.1.3 Hallazgos

A lo largo del ciclo de auditoría se documentaron 12 hallazgos técnicos distribuidos en los cinco componentes evaluados. Su identificación fue progresiva: diez correspondieron a la etapa pre-electoral y dos fueron incorporados durante el seguimiento.

El proceso de seguimiento permitió verificar el estado de las acciones correctivas adoptadas y, en los casos pertinentes, reclasificar el nivel de riesgo en función de los controles compensatorios implementados. Como resultado, cuatro hallazgos fueron subsanados y verificados. Ocho hallazgos se mantienen con criticidad baja al cierre, todos ellos con controles compensatorios vigentes que reducen el riesgo residual a niveles aceptables.

Ninguno de los hallazgos remanentes generó afectaciones operativas verificadas durante la jornada electoral del 8 de marzo de 2026 o posterior.

A continuación, se presenta el estado final de la totalidad de los hallazgos documentados durante el ciclo de auditoría, organizados por componente y según su criticidad.

5.1.3.1 Hallazgos Jurados de votación

La revisión técnica de este componente determinó 2 hallazgos los cuales fueron atendidos de tal forma que se clasifican en estado subsanado y con criticidad baja:

1. Documentación y verificación de controles de arranque seguro (Secure Boot). Estado final: atendido – riesgo bajo
2. Expresión regular potencialmente lenta (ReDoS). Estado final: subsanado.

5.1.3.2 Hallazgos Preconteo

El análisis técnico del componente de Preconteo (Región 1 y Región 2) determinó la mitigación de los riesgos identificados dando como resultado un riesgo residual sin afectación al proceso.

Preconteo · Región 1

1. Documentación y verificación de controles de arranque seguro (Secure Boot). Estado final: atendido – riesgo bajo
2. WebSocket sin autenticación. Estado final: Subsanado

Preconteo · Región 2

1. Controles de ejecución no son efectivos en equipos de Preconteo. Estado final: Subsanado
2. Ausencia de documentación y verificación de controles de arranque seguro (Secure Boot). Estado final: atendido – riesgo bajo.

5.1.3.3 Hallazgos Escrutinio

Respecto al componente de Escrutinio, la evaluación determinó que el 100% de los hallazgos remanentes se consolidaron en un nivel de criticidad baja, sin afectación en la confiabilidad de los resultados ni en la estabilidad de la jornada.

1. Documentación y verificación de controles de arranque seguro (Secure Boot). Estado final: atendido – riesgo bajo.
2. Documentación de ayuda y soporte técnico no comprobada. Estado final: atendido – riesgo bajo.
3. Dependencia operativa del personal clave por ausencia de procedimientos documentados en el despliegue de equipos. Estado final: riesgo bajo.
4. Parcial formalización de criterios logísticos y controles de trazabilidad de los equipos. Estado final: riesgo bajo.

5.1.3.4 Hallazgos Consolidación y divulgación

En este componente se consolidó como subsanado el único hallazgo técnico.

1. Uso de criptografía débil y secretos hardcoded para cifrado. Estado final: subsanado.

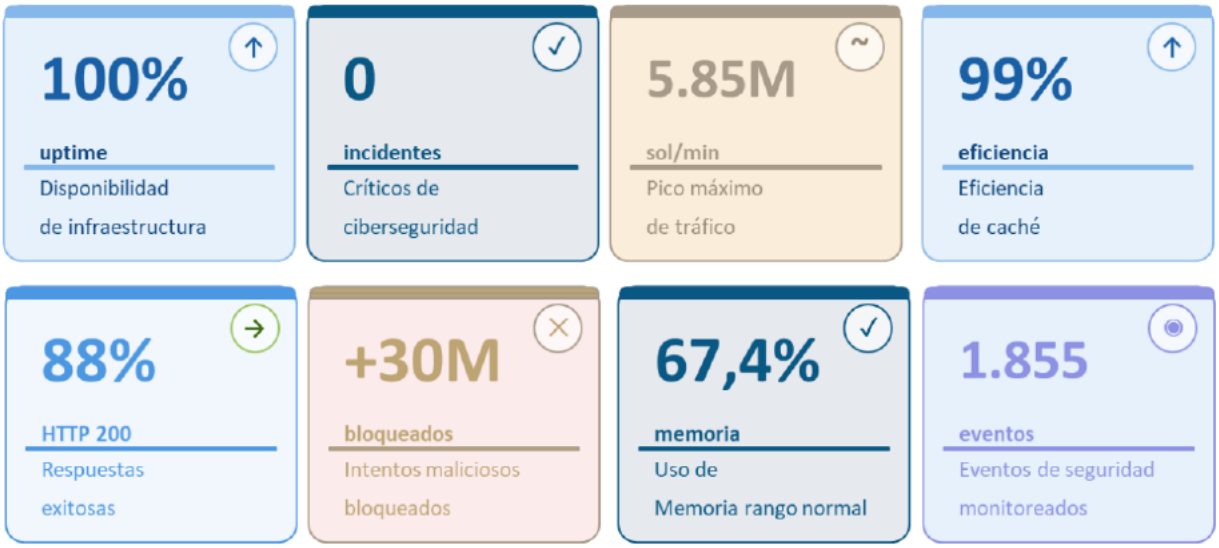
5.1.3.5 Hallazgos Infraestructura tecnológica

En lo referente al componente de Infraestructura Tecnológica, se determinó la mitigación del único hallazgo identificado.

1. Ausencia de uso de Public Key Infrastructure (PKI) para comunicaciones internas. Estado final: atendido – riesgo bajo

5.2 Resultado de los indicadores de desempeño — Jornada electoral

El análisis del rendimiento tecnológico durante la jornada del 8 de marzo de 2026 ratifica la estabilidad y la adecuada capacidad de respuesta de los sistemas implementados. La plataforma operó al 100% de disponibilidad, neutralizó intentos de acceso indebido mediante el bloqueo de más de 30 millones de consultas maliciosas y procesó eficazmente picos de carga de hasta 5.85 millones de solicitudes por minuto, garantizando un 88% de interacciones atendidas correctamente y sin afectaciones en los servicios. Todos los parámetros se mantuvieron dentro de rangos de operación normal:



Indicador	Valor registrado	Interpretación técnica
Disponibilidad de la infraestructura	100%	Sin interrupciones de servicio durante todo el período de análisis
Incidentes críticos de ciberseguridad	0	Ningún evento evolucionó a incidente crítico ni comprometió la operación del sistema
Pico máximo de tráfico	5.857.046 solicitudes/minuto	Registrado a las 19:15 hrs en el portal de resultados (resultados.registraduria.gov.co)
Eficiencia de caché CDN	99%	Solo el 1% de las solicitudes llegó al servidor de origen; el 99% fue servido desde nodos perimetrales (edge)
Tasa de respuestas exitosas (HTTP 200)	88%	Nivel de calidad operacional satisfactorio y consistente con los estándares del servicio
Solicitudes bloqueadas por WAF	Más de 30.000.000	Tráfico automatizado, bots de scraping y ataques de velocidad bloqueados sin impacto en usuarios legítimos
Errores HTTP 5xx registrados	270 en total	Cantidad mínima frente al volumen total de solicitudes procesadas; no representó degradación del servicio
Eventos de seguridad monitoreados (SOC)	1.855 eventos notables	Todos gestionados oportunamente; ninguno evolucionó a incidente crítico
Promedio de eventos por segundo (eps)	5.799 eps (pico: 57.390 eps)	Monitoreo activo durante el período 00:00–22:00 hrs del 8 de marzo
Uso de memoria — Infraestructura AWS	67,4%	Dentro de los rangos normales; sin afectación al servicio

VI. ANÁLISIS TÉCNICO GLOBAL

El proceso integral de auditoría aplicado sobre los componentes de Jurados de Votación, Preconteo, Escrutinio, Consolidación y Divulgación e Infraestructura Tecnológica permitió identificar un escenario general de madurez operativa y tecnológica favorable, caracterizado por una adecuada estabilidad funcional, controles compensatorios efectivos y una capacidad de respuesta consistente durante la jornada electoral.

El análisis consolidado evidencia que la arquitectura tecnológica evaluada mantuvo condiciones satisfactorias de operación, soportadas en prácticas estructuradas de desarrollo de software, mecanismos de control y monitoreo, y capacidades de continuidad operacional. De forma transversal, se observó la existencia de metodologías formales de gestión del ciclo de vida del software, esquemas de control de cambios, procesos de pruebas alineados con buenas prácticas y mecanismos orientados a preservar la integridad y disponibilidad de los sistemas críticos.

Desde la perspectiva de gobernanza tecnológica, se constató un nivel relevante de formalización en componentes relacionados con DevSecOps, custodia del código fuente, documentación técnica, parametrización de aplicativos y trazabilidad de versiones. Asimismo, la existencia de capacidades de monitoreo centralizado, integración con SOC institucional y controles perimetrales evidenció un enfoque preventivo orientado a la resiliencia operativa y la ciberseguridad.

En términos de infraestructura, la evaluación permitió verificar la existencia de centros de datos redundantes, monitoreo continuo de eventos de seguridad, matrices de riesgo tecnológico y documentación asociada a políticas de seguridad de la información. La solución tecnológica implementada presentó capacidades adecuadas para soportar altos volúmenes de procesamiento y tráfico concurrente durante la jornada electoral, manteniendo estabilidad y continuidad de los servicios.

No obstante, el análisis técnico también permitió identificar observaciones las cuales en algunos casos se presentan de igual forma en varios componentes. Las observaciones realizadas versan principalmente en temas de:

- Fortalecimiento documental.
- Versiones de software en uso.
- Documentación de procedimientos de hardening.
- Programas de capacitación y transferencia de conocimiento.
- Pruebas de vulnerabilidades y pruebas de penetración.
- Documentación en procedimientos operativos, continuidad y gobernanza técnica.
- Oportunidades de fortalecimiento en controles de seguridad aplicativa e infraestructura.

A nivel de seguridad de aplicaciones, se identificaron elementos específicos que requieren fortalecimiento preventivo, particularmente relacionados con sanitización de componentes web, almacenamiento seguro de tokens, parametrización de consultas, manejo de autenticación y endurecimiento de configuraciones. Sin embargo, dichas situaciones no derivaron en afectaciones verificadas sobre la integridad de los resultados electorales ni sobre la continuidad operativa de los sistemas auditados.

Respecto a los hallazgos técnicos, el comportamiento general del ciclo de auditoría evidencia una adecuada capacidad de mitigación y respuesta institucional. De los doce hallazgos identificados, cuatro fueron completamente subsanados y ocho permanecieron clasificados con nivel de riesgo bajo. Hay hallazgos con controles compensatorios vigentes que reducen el riesgo residual a niveles aceptables. El seguimiento efectuado permitió verificar la implementación de medidas correctivas y la reducción progresiva de exposición en los componentes evaluados.

Los hallazgos remanentes se relacionan principalmente con aspectos de formalización documental, fortalecimiento de controles de arranque seguro, continuidad operativa y estandarización de procedimientos técnicos, sin evidenciar afectaciones directas sobre la estabilidad funcional de la operación electoral.

Desde la perspectiva operacional, los indicadores de desempeño observados durante la jornada electoral del 8 de marzo de 2026 ratifican la capacidad de respuesta de la infraestructura tecnológica. La disponibilidad del 100%, la ausencia de incidentes críticos de ciberseguridad, la mitigación de más de 30 millones de solicitudes maliciosas y la estabilidad observada frente a picos de tráfico superiores a 5.8 millones de solicitudes por minuto evidencian un comportamiento consistente de los mecanismos de protección, distribución de carga y monitoreo.

La eficiencia del esquema CDN, el bajo volumen de errores HTTP 5xx frente al total de transacciones procesadas y la adecuada gestión de eventos de seguridad desde el SOC permiten concluir que los sistemas mantuvieron condiciones adecuadas de disponibilidad, desempeño y resiliencia durante la etapa más crítica de la operación electoral.

En términos globales, el análisis técnico consolidado permite determinar que:

- Los sistemas evaluados operaron bajo condiciones funcionales estables y controladas.
- Los mecanismos de seguridad, monitoreo y continuidad resultaron suficientes para sostener la operación electoral.
- Hay riesgos residuales identificados que permanecen acotados y controlados mediante controles compensatorios.
- Las observaciones y hallazgos remanentes corresponden principalmente a oportunidades de fortalecimiento preventivo y maduración documental.
- No se evidenciaron afectaciones verificadas sobre la integridad de los resultados electorales, la disponibilidad de los sistemas ni la continuidad de la operación.

Finalmente, se considera técnicamente recomendable mantener un proceso continuo de fortalecimiento enfocado en actualización tecnológica, endurecimiento de plataformas, formalización documental, automatización de monitoreo predictivo y consolidación de capacidades de ciberseguridad, con el propósito de incrementar los niveles de resiliencia y sostenibilidad operativa para futuros procesos electorales.

VII. CONCEPTO FINAL · DICATMEN DE AUDITORÍA DE SISTEMAS

Con fundamento en la evidencia técnica y documental obtenida durante el desarrollo de la Auditoría de Sistemas, y dentro del alcance evaluado en las tres etapas del ciclo electoral —pre-electoral, jornada electoral y post-electoral—, se emite el presente concepto final.

El dictamen se sustenta en los siguientes fundamentos técnicos verificados:

- La revisión técnica y documental confirma la operatividad de la infraestructura tecnológica sin afectaciones en la continuidad de los servicios.
- Los hallazgos de criticidad alta o media identificados fueron atendidos y subsanados. Hay hallazgos remanentes de riesgo bajo que disponen de controles compensatorios vigentes lo que mantiene el riesgo residual en niveles aceptables.
- Se constató la implementación de controles técnicos y de gobernanza en los ámbitos de desarrollo de software seguro, aseguramiento de calidad, custodia del código fuente, continuidad operativa, seguridad perimetral y monitoreo continuo, que reflejan un nivel adecuado de madurez para la operación de sistemas electorales de esta escala y criticidad.
- Todos los componentes evaluados funcionaron adecuadamente cumpliendo con el propósito para el que fueron contratados. La evaluación frente a los criterios contractuales, técnicos y de buenas prácticas internacionales aplicados no evidenció incumplimientos de materialidad que comprometieran la transparencia, integridad, disponibilidad o confiabilidad general del proceso electoral.

En razón de lo anterior, se genera el siguiente dictamen final de auditoría a los sistemas para las Elecciones al Congreso y Consultas Populares 2026:

DICTAMEN: FAVORABLE

Con fundamento en la evidencia técnica y documental obtenida durante el desarrollo de la Auditoría de Sistemas, y dentro del alcance evaluado, se concluye que los sistemas de información y la infraestructura tecnológica auditados para el proceso de Elecciones al Congreso de la República realizadas el 8 de marzo de 2026 operaron con un nivel de implementación, cumplimiento y confiabilidad satisfactorio.

Se constató la implementación de controles técnicos, mecanismos de seguridad y procedimientos operativos que contribuyeron al adecuado funcionamiento de los sistemas electorales en sus tres etapas. La infraestructura tecnológica mantuvo disponibilidad continua durante la jornada electoral, respondió satisfactoriamente al incremento significativo de la demanda y logró neutralizar múltiples intentos de acceso indebido o tráfico automatizado sin afectar la operación del proceso.

No se identificaron situaciones de materialidad que comprometieran la transparencia, integridad, disponibilidad o confiabilidad general del proceso electoral auditado, sin perjuicio de los hallazgos, observaciones y recomendaciones de mejora formulados en el desarrollo del ejercicio auditor, y cuya atención se recomienda mantener como prioridad en el marco de la mejora continua del ecosistema tecnológico electoral.

7.1 Estado de independencia de la auditoría

La Auditoría de Sistemas fue ejecutada con independencia técnica y objetividad, conforme a los principios de la auditoría y los estándares internacionales aplicables. Durante el desarrollo del encargo:

- No se evidenciaron restricciones que comprometieran la independencia del equipo auditor en la emisión de sus conclusiones.
- Las conclusiones formuladas se sustentan exclusivamente en la evidencia técnica y documental recopilada durante las actividades de campo.
- El equipo auditor mantuvo separación funcional respecto de los operadores y ejecutores del proceso electoral.

En consecuencia, se considera que la independencia y objetividad del ejercicio auditor se preservaron durante todas las etapas del proceso.

IIDH / CAPEL