IIDH / CAPEL

INSTITUTO INTERAMERICANO DE DERECHOS HUMANOS
CENTRO DE ASESORÍA Y PROMOCIÓN ELECTORAL

# AUDITORÍA DE SISTEMAS

## AUDITORÍA EXTERNA INTERNACIONAL

*Elecciones Presidente y Vicepresidente de la República 2026,*
*Registraduría Nacional del Estado Civil, Colombia*

# INFORME PRE-ELECTORAL DE AUDITORÍA

28 de mayo, 2026

Elección Presidencial

# INFORME PRE-ELECTORAL

Elección Presidencial

# CONTENIDO

# I. INTRODUCCIÓN

En el marco del proceso electoral correspondiente a las elecciones de Presidente y Vicepresidente de la República previstas para el año 2026, el Instituto Interamericano de Derechos Humanos, a través de su Centro de Asesoría y Promoción Electoral (IIDH/CAPEL), desarrolla la Auditoría Internacional a los Sistemas de Información involucrados en la organización, procesamiento, consolidación y divulgación de resultados electorales, conforme a las disposiciones técnicas definidas en el Anexo Técnico del Convenio de Cooperación Internacional suscrito con la Registraduría Nacional del Estado Civil.

La presente auditoría tiene como propósito evaluar de manera integral las condiciones de eficiencia, seguridad, integridad, disponibilidad, trazabilidad y confiabilidad de los sistemas de información y componentes tecnológicos utilizados durante las distintas etapas del proceso electoral presidencial. Para ello, se ejecuta una revisión técnica especializada sobre los sistemas críticos asociados al sorteo de jurados de votación, procesamiento de preconteo, escrutinios, consolidación y divulgación de resultados, así como sobre la infraestructura tecnológica que soporta la operación electoral.

El presente Informe Pre-Electoral constituye un producto formal del proceso de auditoría para la elección presidencial y documenta el estado inicial de situación de los sistemas auditados, incluyendo el contexto técnico-operativo, el análisis de riesgos, la revisión documental, la evaluación de arquitectura y seguridad.

La auditoría se desarrolla bajo principios de independencia, confidencialidad, objetividad y rigurosidad técnica, mediante la participación de especialistas internacionales en auditoría de sistemas electorales, ciberseguridad, infraestructura tecnológica, y gestión de procesos críticos, con experiencia en procesos electorales de alta complejidad.

# II. ANTECEDENTES

La Registraduría Nacional del Estado Civil, en el marco de la organización de los procesos electorales nacionales de 2026, identificó la necesidad de contar con un servicio especializado de Auditoría Externa Internacional a los sistemas de información involucrados en las elecciones de Congreso de la República y Fórmula Presidencial.

Como parte de dicho proceso, se definió un modelo integral de evaluación técnica orientado a verificar los sistemas de información y componentes tecnológicos utilizados para soportar las operaciones electorales críticas, incluyendo los mecanismos de transmisión, procesamiento, consolidación y divulgación de resultados electorales.

El Anexo Técnico del Convenio establece que la auditoría debe desarrollarse mediante cuatro etapas principales: planificación, trabajo de campo, informe de hallazgos y seguimiento, incorporando revisiones de software, seguridad informática, infraestructura tecnológica y procesos operativos asociados a los sistemas electorales.

En cumplimiento de dichas disposiciones, se ejecutó previamente la auditoría correspondiente al proceso electoral de Congreso de la República, en la que se desarrollaron actividades de revisión documental, validación funcional, análisis de seguridad, verificación de infraestructura y evaluación de controles operativos sobre los sistemas electorales implementados para dicha elección.

Tomando como referencia los resultados obtenidos en la auditoría realizada durante las elecciones de Congreso y considerando las particularidades operativas y de criticidad propias de la elección presidencial, se da inicio al proceso de auditoría correspondiente a las elecciones de Presidente y Vicepresidente de la República, manteniendo el enfoque de revisión integral definido en el alcance contractual y técnico de la auditoría internacional.

La presente fase pre-electoral comprende el análisis de los sistemas y componentes tecnológicos que soportarán el proceso electoral presidencial, con énfasis en la identificación de riesgos, validación de controles, revisión de capacidades operativas y evaluación de las condiciones técnicas requeridas para garantizar la continuidad, integridad y seguridad de la operación electoral.

## III. OBJETIVOS DE LA AUDITORÍA

Los objetivos definidos para la presente Auditoría Externa Internacional constituyen la base orientadora para el desarrollo de las actividades de evaluación técnica aplicadas a los sistemas de información, componentes tecnológicos e infraestructura que soportan el proceso electoral de Presidente y Vicepresidente de la República 2026.

Su definición permite establecer los criterios bajo los cuales se desarrollan las revisiones funcionales, operativas y de seguridad sobre los distintos componentes auditados, facilitando el análisis de las capacidades tecnológicas implementadas, la efectividad de los controles existentes, la identificación de riesgos y vulnerabilidades, así como la valoración del nivel de preparación y confiabilidad de los sistemas involucrados en la operación electoral.

Asimismo, los objetivos de auditoría proporcionan el marco de referencia para la emisión de observaciones, hallazgos y recomendaciones técnicas derivadas del análisis de evidencias y de las actividades de validación ejecutadas durante las distintas etapas del proceso auditor.

### 3.1 Objetivo general

Verificar y evaluar la eficiencia, eficacia, integridad, disponibilidad y seguridad de los sistemas de información y recursos tecnológicos involucrados en el proceso electoral presidencial 2026, mediante la ejecución de una auditoría técnica especializada sobre los componentes críticos del ecosistema electoral.

### 3.2 Objetivos específicos

1. Evaluar la arquitectura funcional y tecnológica de los sistemas electorales involucrados en el proceso presidencial.
2. Verificar la existencia y aplicación de controles de seguridad informática orientados a garantizar la confidencialidad, integridad y disponibilidad de la información electoral.
3. Revisar los procesos de desarrollo, versionamiento y control de cambios implementados sobre los sistemas auditados.
4. Analizar los mecanismos de trazabilidad, procesamiento y consolidación de la información electoral.
5. Validar las capacidades operativas de la infraestructura tecnológica y de los servicios de soporte asociados al proceso electoral.
6. Identificar riesgos técnicos, vulnerabilidades, debilidades de control y posibles exposiciones que puedan afectar la operación electoral.
7. Emitir observaciones y recomendaciones técnicas orientadas a la implementación de acciones preventivas y correctivas antes de la jornada electoral.

# IV. ALCANCE DE LA AUDITORÍA DE SISTEMAS

La auditoría comprende la revisión técnica y funcional de los sistemas de información, procesos operativos y componentes tecnológicos implementados para soportar las elecciones de Presidente y Vicepresidente de la República 2026.

El alcance incluye actividades de auditoría de software, auditoría de seguridad informática, auditoría de procesos y auditoría de infraestructura tecnológica, considerando tanto los ambientes de operación como los mecanismos de soporte, monitoreo y continuidad de los servicios electorales.

Los sistemas de información incluidos dentro del alcance de la auditoría son los siguientes:

- Sistema para Sorteo de Jurados de Votación.
- Sistema para el Procesamiento Electrónico de Datos Electorales (Preconteo) y Comunicaciones.
- Sistema para la realización de Escrutinios.
- Infraestructura Tecnológica – Plataforma de Seguridad Transversal para Soporte Electoral.
- Sistema de Consolidación y Divulgación de Resultados Electorales.

Durante la fase pre-electoral, el alcance se concentra en la revisión documental, análisis de arquitectura, evaluación de controles de seguridad, validación de procesos, análisis de capacidades operativas y levantamiento técnico de información.

La auditoría se desarrolla bajo un enfoque basado en riesgos con estándares internacionales de auditoría de sistemas, seguridad de la información y evaluación de procesos críticos, estructurándose en cuatro etapas principales: planificación, trabajo de campo, presentación de informes y seguimiento.

# V. DELIMITACIÓN TEMPORAL DEL ENCARGO

La información incorporada en este documento corresponde al período de planificación y revisión desarrollado previo a la jornada electoral presidencial, etapa en la cual se efectuaron labores de levantamiento técnico, análisis documental, evaluación de arquitectura tecnológica, revisión de controles de seguridad, validación de procesos operativos y recopilación de evidencias sobre los sistemas objeto de auditoría.

En esta fase se realizaron, entre otras actividades, sesiones técnicas de coordinación con las áreas responsables y contratistas involucrados en los distintos sistemas auditados, revisión de documentación funcional y técnica, análisis de diagramas de infraestructura y red, evaluación de capacidades operativas, verificación de mecanismos de seguridad informática, revisión de código fuente de los sistemas y análisis de los procedimientos definidos para la operación de los sistemas electorales.

> Los resultados contenidos en este informe reflejan el estado de situación observado durante la etapa pre-electoral evaluada y no constituyen una conclusión definitiva sobre la totalidad del proceso de auditoría. Las verificaciones adicionales, nuevas evidencias, validaciones técnicas posteriores y actividades de seguimiento que se ejecuten en etapas subsiguientes serán incorporadas en los informes correspondientes, conforme al avance de la auditoría y al cronograma establecido.

La delimitación temporal aquí definida se circunscribe exclusivamente al período de ejecución de las actividades documentadas en el presente informe. No obstante, dicha delimitación no limita la capacidad de la auditoría para analizar eventos, configuraciones, registros, evidencias o procedimientos generados con anterioridad o posterioridad al período señalado, cuando ello resulte necesario para sustentar adecuadamente los análisis técnicos, validar hallazgos o emitir un criterio profesional razonable sobre los sistemas auditados.

# VI. MARCO NORMATIVO Y TÉCNICO

## 6.1 Fundamento Normativo e Institucional

La presente Auditoría Externa Internacional a los Sistemas de Información involucrados en el proceso electoral de Presidente y Vicepresidente de la República 2026 se desarrolla en el marco de las disposiciones establecidas por la Registraduría Nacional del Estado Civil, el Convenio No. 098 de 2025 y el respectivo Anexo Técnico suscrito para la prestación de servicios especializados de Auditoría Externa y Auditoría a los Sistemas de Información asociados a los procesos electorales nacionales de 2026.

El ejercicio auditor se fundamenta en principios de independencia, objetividad, confidencialidad, trazabilidad y rigor técnico, orientados a garantizar que las actividades de evaluación sean desarrolladas bajo criterios verificables y técnicamente sustentados, preservando en todo momento la imparcialidad y autonomía del proceso de auditoría.

El marco institucional de referencia contempla la coordinación permanente entre la Auditoría Externa Internacional, la Registraduría Nacional del Estado Civil, las áreas técnicas responsables de los sistemas auditados y los distintos contratistas vinculados a la operación electoral, con el propósito de facilitar el acceso a la información, la validación de evidencias y el seguimiento oportuno de observaciones y recomendaciones derivadas del proceso auditor.

## 6.2 Referencias Normativas Aplicables

La ejecución de la auditoría considera como marco de referencia las disposiciones legales, contractuales y regulatorias aplicables a la protección de la información, operación de sistemas críticos y tratamiento de datos asociados al proceso electoral.

En materia de protección y tratamiento de información, se consideran las disposiciones establecidas en la Ley 1581 de 2012 sobre Protección de Datos Personales, particularmente en lo relacionado con la confidencialidad, custodia, tratamiento y protección de la información suministrada durante el desarrollo de las actividades de auditoría. De igual forma, se toman como referencia las disposiciones de la Ley 1273 de 2009 relacionadas con la protección de la información y los datos, así como los mecanismos orientados a prevenir afectaciones sobre sistemas informáticos y activos digitales críticos.

El proceso auditor se desarrolla igualmente bajo las obligaciones de confidencialidad definidas contractualmente entre las partes intervinientes, garantizando que la información técnica, operativa y documental suministrada por la Registraduría Nacional del Estado Civil y sus contratistas sea utilizada exclusivamente para los fines asociados a la evaluación técnica contemplada dentro del objeto contractual.

Desde la perspectiva técnica y operativa, la auditoría toma como referencia las disposiciones definidas en el Anexo Técnico del proceso contractual, el cual establece el alcance funcional de los sistemas auditados, las etapas de ejecución de la auditoría, los componentes tecnológicos sujetos a evaluación y las actividades mínimas requeridas para las revisiones de software, seguridad informática, infraestructura tecnológica y procesos operativos.

## 6.3 Marco técnico · Estándares y Buenas Prácticas

La presente auditoría tomó como referencia los siguientes estándares y marcos internacionalmente reconocidos en materia de auditoría, gobierno, gestión y seguridad de tecnologías de información, con el propósito de desarrollar una evaluación alineada con buenas prácticas aplicables a infraestructuras tecnológicas críticas y sistemas de alta sensibilidad operativa.

### COBIT 2019 (Control Objectives for Information and Related Technologies)

Marco de gobierno y gestión de TI emitido por ISACA. Proporciona criterios para la alineación estratégica de la tecnología con los objetivos institucionales, la gestión de riesgos tecnológicos, el control de procesos de TI y la medición de su desempeño. En el contexto de la auditoría, COBIT orienta la evaluación de los procesos de gobierno sobre los sistemas electorales, incluyendo la gestión de cambios, control de configuraciones, gestión de incidentes y continuidad del servicio.

### ITAF – Information Technology Assurance Framework (ISACA)

Marco metodológico de referencia para la práctica profesional de auditoría de sistemas de información. Establece estándares, directrices y procedimientos para la planificación, ejecución, documentación y reporte de auditorías de TI. La aplicación de ITAF garantiza que el proceso auditor se desarrolle bajo criterios de independencia, objetividad, competencia profesional y rigor técnico, proporcionando la estructura metodológica para la identificación, evaluación y clasificación de hallazgos.

### ISO/IEC 19011 – Directrices para la Auditoría de Sistemas de Gestión

Norma internacional que establece los principios, la gestión de programas de auditoría y la conducción de auditorías de sistemas de gestión. Orienta aspectos relacionados con la competencia de los auditores, la planificación de auditorías, la recopilación y verificación de evidencias, los criterios de evaluación y la elaboración de informes. Se aplica para estructurar el proceso auditor bajo un marco metodológico internacionalmente reconocido.

### ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información

Norma internacional que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Proporciona el marco de referencia para evaluar la existencia y efectividad de los controles de seguridad implementados sobre los sistemas electorales, considerando la protección

de la confidencialidad, integridad y disponibilidad de la información electoral procesada.

### ISO/IEC 27002 – Controles de Seguridad de la Información

Norma que proporciona directrices para la implementación de controles de seguridad de la información. Establece un catálogo de controles de seguridad organizacionales, de personas, físicos y tecnológicos que sirven como referencia para evaluar la adecuación y efectividad de las medidas de seguridad implementadas en los sistemas electorales. Se utiliza para verificar controles relacionados con gestión de accesos, criptografía, seguridad en redes, operaciones de TI y gestión de incidentes de seguridad.

### ISO/IEC 27005 – Gestión de Riesgos de Seguridad de la Información

Norma que proporciona directrices para la gestión de riesgos de seguridad de la información. Orienta los procesos de identificación, análisis, evaluación y tratamiento de riesgos tecnológicos, fundamentando el enfoque basado en riesgos aplicado durante la evaluación. Se utiliza para determinar el nivel de exposición de los sistemas electorales ante amenazas y vulnerabilidades identificadas, así como para priorizar las acciones correctivas y preventivas recomendadas.

### OWASP – Open Web Application Security Project

Marco de referencia internacional para la seguridad de aplicaciones. Proporciona metodologías, herramientas y directrices para la identificación y mitigación de vulnerabilidades en aplicaciones de software, incluyendo las referencias OWASP Desktop App Security y Top 10. Se aplica durante las pruebas de penetración, análisis de vulnerabilidades y revisión de seguridad de los sistemas electorales, considerando las particularidades técnicas de las aplicaciones de escritorio y servicios web involucrados en el proceso electoral.

### NIST Cybersecurity Framework (CSF)

Marco de ciberseguridad desarrollado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos. Estructura la evaluación de la ciberseguridad en torno a cinco funciones principales: Identificar,

Proteger, Detectar, Responder y Recuperar. En el contexto de la auditoría, el NIST CSF orienta la evaluación de la madurez de los controles de ciberseguridad implementados, la capacidad de detección y respuesta ante incidentes y la resiliencia operativa de la infraestructura tecnológica electoral.

La utilización de estos referentes permite estructurar un modelo de evaluación basado en prácticas internacionalmente aceptadas para la gestión, control y auditoría de tecnologías de información, orientado a verificar condiciones de eficiencia, confiabilidad, trazabilidad, disponibilidad, integridad y seguridad sobre los sistemas y componentes tecnológicos involucrados en el proceso electoral presidencial.

# VII. METODOLOGÍA DE AUDITORÍA

La auditoría a los sistemas de información involucrados en el proceso electoral de Presidente y Vicepresidente de la República 2026 fue estructurada de manera integral orientada a verificar no solamente el funcionamiento individual de los sistemas auditados, sino también las condiciones de seguridad, interoperabilidad, trazabilidad, resiliencia y continuidad operativa del ecosistema tecnológico que soporta el proceso electoral presidencial.

El modelo metodológico adoptado se fundamenta en un enfoque basado en riesgos y en la aplicación de prácticas internacionalmente reconocidas en materia de auditoría de sistemas, seguridad de la información, gestión de infraestructura tecnológica y evaluación de procesos críticos, permitiendo desarrollar una evaluación multidisciplinaria sobre los distintos componentes tecnológicos, operativos y procedimentales involucrados en la organización y ejecución del proceso electoral.

Bajo este enfoque, la auditoría incorpora revisiones relacionadas con integridad, control de versiones, trazabilidad de operaciones, mecanismos de monitoreo, gestión de vulnerabilidades, controles de seguridad lógica y física, disponibilidad de servicios, continuidad operativa, autenticidad de software, análisis de código fuente, soporte técnico y procedimientos de despliegue y operación tecnológica.

De conformidad con lo establecido en el Anexo Técnico contractual, la metodología de auditoría se estructura en cuatro etapas principales: planificación, trabajo de campo, presentación de informes y seguimiento, las cuales se detallan a continuación

## 7.1 Etapas de la auditoría

Las cuatro etapas de la auditoría se desarrollan de manera progresiva y articulada durante las distintas fases del proceso electoral, garantizando cobertura integral sobre todos los sistemas y componentes tecnológicos involucrados.

### 7.1.1 Etapa de Planificación

La etapa de planificación corresponde al proceso inicial de organización, levantamiento técnico y análisis de los sistemas objeto de auditoría, cuyo propósito consiste en definir el alcance operativo de las evaluaciones, identificar los riesgos asociados a cada sistema y establecer las actividades técnicas necesarias para el desarrollo del proceso auditor.

Como parte de las actividades de planificación, se desarrollan reuniones técnicas con las áreas responsables y contratistas involucrados en los diferentes sistemas, con el propósito de presentar los objetivos de auditoría, coordinar las actividades de evaluación, establecer cronogramas de trabajo y definir los mecanismos de suministro y validación de información.

En esta fase también se ejecuta un análisis del estado de situación de los sistemas auditados, orientado a identificar condiciones de riesgo, brechas técnicas, dependencias operativas y aspectos críticos que requieren validación posterior durante el trabajo de campo. Dicho análisis contempla la revisión de características funcionales, diseño de infraestructura, mecanismos de seguridad, capacidades operativas y condiciones de integridad, disponibilidad y confidencialidad de la información procesada.

Para cada componente de auditoría (software, seguridad, procesos, infraestructura), se estableció la planificación detallada que define los objetivos del trabajo a realizar, así como las pruebas a ejecutar para cada sistema definido en el alcance de la auditoria.

### 7.1.2 Trabajo de Campo

La etapa de trabajo de campo comprende la ejecución de evaluaciones técnicas especializadas orientadas a verificar el comportamiento funcional, operativo y de seguridad de los sistemas auditados, según las actividades definidas en la etapa de planificación, mediante la aplicación de pruebas, revisiones técnicas, validaciones operativas y análisis de evidencias sobre los distintos sistemas y componentes tecnológicos involucrados en el proceso electoral.

Durante esta etapa se desarrollan actividades conforme lo definido para cada componente de la auditoría: software, seguridad, procesos e infraestructura tecnológica, permitiendo evaluar integralmente los mecanismos de control implementados sobre los sistemas electorales y su capacidad para garantizar condiciones adecuadas de integridad, disponibilidad, trazabilidad y continuidad operativa.

#### 7.1.2.1 Auditoría de Software

La auditoría de software se orienta a evaluar los procesos de diseño, desarrollo, implementación y operación de los sistemas electorales auditados, con el propósito de verificar que las aplicaciones cumplan adecuadamente las funcionalidades requeridas para la operación del proceso electoral.

Como parte de la planificación para este componente de auditoría se establecieron las siguientes actividades específicas aplicables a cada sistema incluido en el alcance:

Actividades:

1. Verificar la trazabilidad e integridad de la versión de software desplegada en producción, asegurando que corresponde exactamente al código fuente auditado.

2. Verificar que la lógica de negocio implementada en el software para el procesamiento de los datos sea correcta, consistente y conforme a las reglas funcionales definidas, garantizando la exactitud de los resultados generados.

3. Verificar que los mecanismos de almacenamiento y persistencia de datos del software garanticen la integridad, consistencia y no alteración de la información, asegurando que los datos se registran correctamente y no sufren modificaciones no autorizadas en los repositorios correspondientes.

4. Verificar que el software ha sido sometido a procesos formales de aseguramiento de calidad (QA), incluyendo pruebas funcionales, no funcionales y de rendimiento, garantizando el correcto funcionamiento de todas sus funcionalidades. Asimismo, validar que la arquitectura del sistema es adecuada, escalable y resiliente, soportando de manera eficiente la carga transaccional y los niveles de demanda esperados.

5. Verificar que los procesos de gestión y control de cambios se encuentren formalmente implementados y operativos, garantizando la trazabilidad completa de los cambios (desde su solicitud hasta su despliegue), así como la existencia de un historial auditado y consistente, gestionado mediante un esquema adecuado de versionamiento del software (control de versiones, ramas, etiquetado y registros de integración).

### Revisión documental:

Se lleva a cabo la siguiente revisión documental según el caso para cada sistema:

- Código fuente del sistema alojado en GitHub.
- Diagramas de arquitectura
  - Detalle de infraestructura en la nube, microservicios y zonas de disponibilidad.

  - Preconteo Zona 1: Detalle de infraestructura en la nube y zonas de disponibilidad.
  - Preconteo Zona 2: Detalle de infraestructura en la nube, y On-Premise con sus microservicios y zonas de disponibilidad.
- Metodología de gestión: Configuración de épicas, historias, tareas y sprints en Jira / Azure DevOps / Microsoft Planner según el caso.
- Anexo Técnico del contrato: Documento de requerimientos entre la Registraduría Nacional y la UT ILE 2026.
- Diagrama de GitFlow: Modelo de gestión de ramas y control de versiones.
- Gestión de requerimientos: Historial de tickets y formularios de requerimiento en Jira / Azure DevOps según el caso.

Pruebas ejecutadas:

Dentro de las pruebas realizadas, se lleva a cabo:

1. Revisión de la metodología de Control de Calidad: su objetivo es comprobar el cumplimiento de los siguientes objetivos:

   - Revisión de los 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.

   Para esto se lleva a cabo la revisión de la metodología de aseguramiento y control de calidad aplicada durante el proceso de desarrollo del sistema. Se valida la siguiente información:

   - Código fuente del sistema.
   - Diagrama de la arquitectura del sistema.
   - Diagrama del modelo DevOps implementado según sea el caso.
   - Tickets en la plataforma Jira o Azure DevOps según sea el caso.

   La revisión de la metodología de control de calidad permite asegurar el proceso de desarrollo y evitar los siguientes riesgos:

- Liberación de software con errores funcionales.
- Fallas de integración entre componentes del sistema
- Vulnerabilidades de seguridad en el código fuente
- Inestabilidad operativa en ambientes productivos
- Incumplimiento de requerimientos funcionales y técnicos

2. Revisión de los procedimientos utilizados para el control de cambios: esta revisión tiene como propósito comprobar el cumplimiento de los siguientes objetivos de la auditoría:
   - Que se realiza una adecuada gestión y control de cambios y pruebas.
   - Que los procedimientos de diseño, desarrollo y versionado son adecuados

   Durante la revisión de la metodología de desarrollo de software implementada por la organización, se efectúa el análisis del proceso de control y gestión de cambios aplicado a cada sistema.

   Para esta prueba se valida la siguiente información:

   - Código fuente del sistema.
   - Diagrama de la arquitectura del Sistema.
   - Metodología de gestión de proyectos y la de desarrollo de software implementada.

   La revisión del proceso de control de cambios permite asegurar el proceso de desarrollo y evitar los siguientes riesgos:

   - Implementación de cambios no autorizados
   - Pérdida de trazabilidad sobre los cambios realizados.
   - Liberación de funcionalidades con errores
   - Inconsistencias entre requerimientos y desarrollos implementados
   - Afectación de la estabilidad del sistema en producción.

3. Revisión y depuración del código fuente: tiene como propósito comprobar el cumplimiento de los siguientes objetivos de la auditoría:

   - Que las capacidades de parametrización se adecúan a los requerimientos.
   - Análisis los sistemas desde una perspectiva de desarrollo de software de forma que sea posible identificar y determinar posibles funcionalidades defectuosas.
   - Revisión de código fuente.

   Para esta prueba se lleva a cabo el proceso de depuración y revisión técnica del código fuente correspondiente al sistema auditado, esta prueba se ejecuta en conjunto con el líder de desarrollo del sistema, quién además realiza una exposición funcional y técnica de los distintos componentes y servicios que conforman la solución.

   Como parte de la revisión documental se revisa:

   - Código fuente del sistema.
   - Diagrama de arquitectura general de la solución presentado y explicado por parte del equipo de desarrolladores.
   - Metodología de gestión de proyectos y la de desarrollo de software implementada en la herramienta Jira / Azure DevOps según sea el caso.

   La ejecución de actividades de depuración, revisión funcional y validación técnica del código fuente durante una auditoría de software permite mitigar diversos riesgos asociados a la puesta en producción de sistemas críticos, especialmente en plataformas electorales. Entre los principales riesgos potenciales que se logran prevenir se encuentran los siguientes:

   - Errores en la carga y procesamiento de información fuente.
   - Aplicación incorrecta de reglas de operación.
   - Fallos en los algoritmos.

- Inconsistencias entre requerimientos y funcionalidad implementada.
- Errores en la generación de resultados.
- Incidentes operativos posteriores a la liberación en producción.

4. Revisión de la Metodología de Desarrollo Implementada: tiene como propósito comprobar el cumplimiento de los siguientes objetivos de la auditoría:

   - 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 los casos de uso estén completos, detallados y acordes a las necesidades del proceso.

   Para esta prueba se valida la siguiente información:

   - Código fuente del sistema.
   - Diagrama de arquitectura general de las soluciones presentado y explicado por parte del equipo de desarrolladores.
   - Metodología de gestión de proyectos y la de desarrollo de software implementada.
   - Documento con el Anexo Técnico del contrato entre la Registraduría Nacional del Estado Civil y la Unión Temporal Integración Logística Electoral 2026 (UT ILE 2026), los cuales se convierten en los requerimientos para el sistema.

   La revisión de la metodología de desarrollo utilizada para la implementación del sistema permite mitigar diversos riesgos técnicos, operativos y de gestión que podrían impactar negativamente la estabilidad y confiabilidad del sistema en ambiente de producción. Entre

los principales riesgos potenciales que se logran prevenir se encuentran los siguientes:

- Riesgos de implementación de funcionalidades no alineadas con los requerimientos
- Falta de trazabilidad de cambios y requerimientos
- Problemas de calidad derivados de procesos de desarrollo no estructurados
- Riesgos de dependencia operativa o pérdida de conocimiento por falta de un proceso de documentación adecuado

5. Revisión del procedimiento de control de versiones: su propósito es comprobar el cumplimiento de que los procedimientos de diseño, desarrollo y versionado de los sistemas son adecuados. Para esta prueba se valida la siguiente información:

   - Código fuente del sistema.
   - Sistema para el manejo de tickets con nuevos requerimientos según sea el caso (Jira / Azure DevOps)
   - Diagrama del manejo de control de versiones mediante GitFlow según sea el caso.
   - Diagrama del modelo DevOps implementado según sea el caso

   La implementación de un modelo de control de versiones usando GitHub / GItFlow permite reducir riesgos asociados a conflictos de código, pérdida de cambios, liberaciones no controladas, incorporación de funcionalidades no validadas y afectaciones sobre ambientes productivos, proporcionando un marco básico organizado para la administración de versiones y evolución continua de los sistemas desarrollados.

6. Revisión de los métodos utilizados en el almacenamiento y persistencia de los datos del sistema: su propósito es comprobar el cumplimiento de los siguientes objetivos:

- 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.

Durante el proceso de depuración del código fuente y revisión técnica que se realizada con el equipo de desarrollo del sistema, se efectúa el análisis de los mecanismos implementados para la persistencia y gestión de información en las diferentes bases de datos del sistema.

Para esta prueba se valida la siguiente información:

- Código fuente del sistema contenido en el repositorio GitHub.
- Diagrama de la arquitectura del sistema.

La revisión de los métodos utilizados para la persistencia de la información permite asegurar el proceso de desarrollo y evitar los siguientes riesgos:

- Ataques de inyección SQL
- Manipulación o acceso no autorizado a información sensible
- Corrupción o inconsistencia de datos
- Degradación del rendimiento en operaciones masivas
- Indisponibilidad del sistema por fallos en la base de datos

7. Revisión de la arquitectura del Sistema: su propósito es comprobar el cumplimiento de los siguientes objetivos:

- 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.

Para esta prueba se valida la siguiente información:

- Código fuente del sistema contenido en el repositorio Github.
- Diagrama de la arquitectura del sistema.
- Diagrama del modelo DevOps implementado

La implementación de una arquitectura basada en microservicios contenerizados, servicios administrados en la nube y componentes de alta disponibilidad permite alertar de riesgos técnicos y operativos asociados a sistemas críticos de procesamiento electoral, entre estos riesgos están:

- Evitar que la caída de un componente afecte la operación total del sistema.
- Reducir riesgos de indisponibilidad durante procesos críticos o de alta demanda.
- Reducir riesgos asociados a implementaciones incorrectas o cambios no controlados.

#### 7.1.2.2 Auditoría de Seguridad e Infraestructura

La auditoría de seguridad e infraestructura tiene como finalidad evaluar los controles técnicos y organizacionales implementados para garantizar la integridad, disponibilidad y confidencialidad de la información electoral y de la infraestructura tecnológica que soporta la operación de los sistemas auditados, así como evaluar los componentes físicos, lógicos y de comunicaciones que soportan transversalmente la operación de los sistemas electorales auditados.

Dentro de estos componentes de auditoría se desarrollaron las siguientes actividades definidas desde la planificación:

Actividades:

1. Evaluar la integridad, autenticidad y no alteración de los datos electorales y de los sistemas que los procesan, así como la trazabilidad existente sobre software, infraestructura, transacciones críticas y evidencias técnicas durante todo el ciclo electoral.

2. Revisar que se cuente con una plataforma electoral resiliente, disponible y recuperable, capaz de soportar la operación presidencial con continuidad, redundancia, tolerancia a fallos y capacidad suficiente ante escenarios de alta demanda o contingencia.
3. Evaluar si se ha reducido la superficie de exposición y se ha fortalecido la postura de seguridad de la infraestructura y los sistemas electorales, mediante configuraciones seguras, endurecimiento técnico, gestión de parches y controles preventivos y detectivos consistentes.

4. Evaluar si se ha establecido un control robusto de identidades, accesos y trazabilidad operativa, que limite el privilegio a lo estrictamente necesario, permita validar acciones por rol y reduzca el riesgo de uso indebido o manipulación no autorizada durante la elección presidencial.

5. Confirmar que la solución electoral puede ser evaluada técnica y funcionalmente con suficiente profundidad, permitiendo identificar vulnerabilidades, fallas de lógica, debilidades de implementación y riesgos sobre componentes internos y expuestos.

6. Verificar que se gestiona el riesgo tecnológico electoral de manera continua y verificable, priorizando escenarios que puedan comprometer la legitimidad, continuidad, confidencialidad o integridad del proceso presidencial y definiendo tratamientos formales para su mitigación.

Asimismo, se llevó a cabo la siguiente revisión documental:

Revisión documental:

- Inventario actualizado y detallado de hardware, software y equipamiento que intervienen en el proceso electoral, incluyendo servidores, comunicaciones, almacenamiento, backups, licencias y versiones.
- Diagramas actualizados de arquitectura lógica y física, incluyendo topología de red, segmentación, VLAN, enlaces, dependencias y puntos de acceso.
- Descripción técnica de mecanismos de autenticación, integridad y no repudio, incluyendo hash, firma digital, controles criptográficos y autenticación multifactor.
- Políticas y procedimientos de registro, auditoría y retención de logs, incluyendo alcance, tiempos y ubicación. Bitácoras disponibles y evidencia de revisiones periódicas de logs y eventos críticos.
- Políticas de logging específicas para transacciones sensibles y para el sistema electoral.
- Matriz de dimensionamiento y capacidad, incluyendo CPU, RAM, almacenamiento, usuarios concurrentes y TPS.
- Diseño y arquitectura de alta disponibilidad, redundancia y tolerancia a fallos. Acuerdos de nivel de servicio vigentes, incluyendo métricas de disponibilidad y soporte.
- Políticas y planes de respaldo, recuperación ante desastres y continuidad operativa.
- Bitácoras o reportes de pruebas de restauración y recuperación ejecutadas.
- Flujos operativos y procedimientos del servicio de mesa de ayuda.
- Políticas y lineamientos de configuración de BIOS/UEFI y Secure Boot.
- Políticas de hardening, guías de configuración y evidencias de su aplicación.
- Evidencia de parches aplicados o plan formal de actualización de software y sistemas.
- Procedimientos de administración de infraestructura, incluyendo instalación, cambios y mantenimiento.

- Políticas de seguridad de la información y gestión de vulnerabilidades vigentes.
- Inventario de herramientas de seguridad implementadas, incluyendo firewall, WAF, IDS/IPS, EDR, antimalware y SIEM.
- Resultados de pruebas de seguridad previas, incluyendo pentesting, análisis de vulnerabilidades y auditorías.
- Políticas y procedimientos de gestión de usuarios, roles y privilegios.
- Procedimientos de provisión, baja y revisión periódica de accesos.
- Cuentas de usuario en distintos roles y acceso a ambiente funcional de las aplicaciones para la ejecución de las pruebas.
- Acceso a repositorios de código fuente de la solución para ejecución de análisis estático.
- Acceso a un ambiente de depuración que permita seguir el código y la aplicación en ejecución.
- Listado de IPs, dominios y aplicaciones a evaluar, y acceso a la red al equipo del consultor para hacer evaluación de vulnerabilidades en estos activos.
- Procedimientos de gestión de incidentes de seguridad, respuesta y escalamiento.
- Matriz de riesgos tecnológicos actualizada, incluyendo probabilidad, impacto y controles asociados.
- Metodología de gestión de riesgos utilizada.
- Planes de tratamiento de riesgos.

### Pruebas ejecutadas:

Dentro de las pruebas realizadas en materia de seguridad, se llevó a cabo:

1. Verificación de controles de arranque seguro y hardening de endpoints electorales: esta prueba tiene como propósito verificar que los equipos desplegados para el proceso electoral cuentan con controles de arranque seguro y hardening que impidan la ejecución de software no autorizado o la modificación de configuraciones críticas.

Como parte de esta prueba se ejecuta la evaluación de hardening. Las pruebas incluyen: intento de ejecución de software no autorizado, intento de acceso a línea de comandos/shell, intento de ejecución de utilidades del sistema desde rutas no convencionales, intento de modificación de configuraciones críticas del SO, e intento de bypass mediante técnicas de evasión de controles de aplicación (application allowlisting / SRP / WDAC).

Dentro de la revisión documental se revisan las políticas de hardening, guías de configuración BIOS/UEFI y Secure Boot, evidencias de aplicación de controles.

El riesgo potencial que motiva la realización de esta prueba es la ejecución de código malicioso en equipos electorales, modificación no autorizada de configuraciones del sistema, compromiso de la integridad del proceso electoral.

2. Evaluación de controles de disponibilidad y continuidad de la plataforma electoral: esta prueba tiene como propósito verificar que la plataforma electoral cuenta con controles suficientes para garantizar la disponibilidad y continuidad del servicio durante la jornada electoral, incluyendo escenarios de alta demanda y contingencia.

   Como parte de esta prueba se evalúa la capacidad de la plataforma electoral para mantener la disponibilidad del servicio durante la jornada electoral mediante la revisión de: arquitectura de alta disponibilidad, redundancia de componentes críticos, balanceo de carga, mecanismos de failover, planes de recuperación ante desastres (DRP), y procedimientos de continuidad operativa.

   La revisión documental en esta prueba se centra en la arquitectura de alta disponibilidad, SLAs, planes DRP/BCP, procedimientos de failover, métricas de capacidad y dimensionamiento.

El riesgo potencial que motiva la realización de esta prueba es la interrupción del servicio durante la jornada electoral, perdida de datos electorales por falta de redundancia, tiempos de recuperación excesivos ante fallos.

3. Evaluación de hardening, aseguramiento de SO, análisis de vulnerabilidades y pruebas de penetración: tiene como propósito verificar que la superficie de exposición ha sido reducida mediante hardening, gestión de parches y configuraciones seguras en infraestructura y aplicaciones.

   Esta prueba evalúa el nivel de hardening y aseguramiento de los sistemas operativos en equipos electorales representativos. Se ejecuta escaneo autenticado de vulnerabilidades con Tenable Nessus sobre ~80 servidores RHEL 9 en Zona 1 y 4 servidores Debian en Zona 2. Se ejecutan pruebas de penetración tipo caja gris sobre las cuatro plataformas web del ecosistema electoral utilizando OWASP WSTG v4.2 + PTES + ASVS.

   Se revisan las políticas de hardening, listado de IPs y dominios, políticas de gestión de parches, resultados de pruebas de seguridad previas.

   El riesgo potencial que motiva esta prueba es la explotación de vulnerabilidades conocidas en servidores críticos, ejecución remota de código no autenticado, compromiso de datos electorales.

4. Evaluación de controles de identidad, acceso y trazabilidad en sistemas electorales: tiene como propósito verificar que los sistemas electorales implementan controles robustos de identidad y acceso que limiten el privilegio al mínimo necesario y permitan la trazabilidad de acciones por rol.

   Se evaluaron los controles de gestión de identidades y accesos en los sistemas electorales mediante: revisión de mecanismos de autenticación (JWT, reCAPTCHA), políticas de autorización a nivel de

objeto (IDOR), gestión de roles y privilegios en las plataformas web, procedimientos de enrolamiento de equipos en la red y trazabilidad de acciones por rol en los sistemas evaluados.

Se revisan las políticas de gestión de usuarios, roles y privilegios, procedimientos de provisión y baja de accesos y documentación de flujos de autenticación y autorización.

El riesgo potencial que motiva esta prueba es el acceso no autorizado a recursos por deficiencias en autorización (IDOR), escalamiento de privilegios, falta de trazabilidad de acciones críticas, bypass de mecanismos de autenticación.

5. Evaluación técnica profunda mediante SAST, DAST, análisis de vulnerabilidades y pruebas de caja gris: tiene como propósito confirmar que la solución electoral puede ser evaluada con suficiente profundidad para identificar vulnerabilidades, fallas de lógica, debilidades de implementación y riesgos en componentes internos y expuestos.

   Como parte de esta prueba se ejecuta una evaluación técnica profunda de la solución electoral combinando cuatro enfoques complementarios:

   - SAST (SonarQube): análisis estático del Código fuente de todos los componentes.
   - DAST: Debugging e inspección de trafico de red (Wireshark)
   - análisis de vulnerabilidades (Nessus): Escaneo autenticado de ~84 servidores on-premise.
   - Pruebas de caja gris (OWASP WSTG v4.2 + PTES + ASVS): Sobre las 4 plataformas web del ecosistema electoral.

   Dentro de la revisión documental, se revisa código fuente, listado de IPs/dominios, configuración de herramientas de seguridad.

   El riesgo potencial que motiva esta prueba son las vulnerabilidades no detectadas en código fuente, debilidades de implementación en

componentes críticos, fallas de lógica de negocio explotables, riesgo residual no identificado.

6. Evaluación de la gestión de riesgo tecnológico electoral: su propósito es verificar que se gestiona el riesgo tecnológico electoral de manera continua y verificable, con tratamientos formales para riesgos que puedan comprometer el proceso presidencial.

   Para esta prueba se evalúa la gestión de riesgo tecnológico del proceso electoral mediante la correlación de los resultados de todas las pruebas ejecutadas:

   - Riesgos de integridad: Evaluados mediante controles de hash y SAST.
   - Riesgos de disponibilidad: Evaluados mediante revisión de arquitectura y pruebas de caja gris.
   - Riesgos de vulnerabilidades: Evaluados mediante Nessus y pruebas de penetración.
   - Riesgos de acceso no autorizado: Evaluados mediante pruebas de IDOR y bypass de autenticación.

   La revisión documental se centra en la matriz de riesgos tecnológicos, metodología de gestión de riesgos, planes de tratamiento de riesgos, políticas de seguridad y gestión de vulnerabilidades.

   El riesgo potencial que motiva esta prueba son los riesgos tecnológicos no identificados o sin tratamiento formal, priorización inadecuada de la remediación de vulnerabilidades críticas, ausencia de planes de mitigación para escenarios de alto impacto.

Dentro de las pruebas realizadas sobre la infraestructura, se llevan a cabo:

1. Desarrollo del Checklist Técnico del Anexo Técnico del Contrato 049 y 060: tiene como propósito comprobar el cumplimiento de cada uno de

los puntos de los objetivos de la auditoría los cuales están basados en el Anexo Técnico del Contrato 049 y 060.

Para esto se realiza trabajo de campo y se valida el cumplimiento contra una lista de chequeo para establecer su concordancia con los documentos y las configuraciones demostradas en las sesiones técnicas realizadas con el personal asignado, de forma tal que la ejecución de esta prueba esté debidamente sustentada en las evidencias provistas y mostradas.

Con esta verificación se busca validar que no existan incumplimientos documentales, técnicos, procesales o de ejecución como parte de los objetivos de la auditoría para este componente, lo que permite determinar el cumplimiento de lo expresado en el Anexo Técnico del Contrato 049, logrando así que se identifiquen riesgos potenciales.

2. Visita a los Data Centers de Nebula y Monserrate: su propósito es comprobar el cumplimiento de lo solicitado en el Anexo Técnico del Contrato 049 y el 060 con respecto a los Data Centers y las certificaciones de las normas TIA-942 TIER III o superior o ICREA IV o superior.

   Para esto se realiza la visita a los Data Center de Nebula y Monserrate para validar las facilidades y el cumplimiento de las normativas establecidas, donde se estipula que se debe disponer de máximo dos (2) Data centers (Centros de Datos), que cumplan como mínimo con las características contenidos en la norma TIA-942 TIER III o superior o ICREA IV o superior.

   El objetivo de la visita a los data center es validar el cumplimiento documental, procedimental y las certificaciones técnicas, que son parte de los objetivos de la auditoría para este componente.

   El riesgo potencial asociado a esta verificación radica en que el incumplimiento de las condiciones técnicas, operativas y de

certificación exigidas para los Data Centers podría afectar la disponibilidad, continuidad, resiliencia y seguridad de la infraestructura tecnológica que soporta los sistemas electorales críticos. Por esta razón, resulta fundamental verificar que las instalaciones, controles de infraestructura, mecanismos de redundancia y certificaciones asociadas cumplan efectivamente con los estándares establecidos, a fin de establecer oportunamente las medidas correctivas y preventivas necesarias para minimizar riesgos de interrupción, degradación del servicio o afectación sobre la operación de los sistemas electorales.

#### 7.1.2.3 Auditoría de Procesos

La auditoría de procesos se enfoca en la evaluación de los procedimientos operativos y administrativos asociados al uso, soporte y operación de los sistemas electorales, considerando que las tecnologías de información constituyen un medio habilitador para la correcta ejecución de los procesos críticos del proceso electoral.

Esta evaluación contempló las siguientes actividades definidas en la planificación.

**Actividades:**

En esta auditoría se examinó el soporte documental con el propósito de evaluar su funcionamiento y el grado de cumplimiento de los procesos definidos por la organización. El alcance de la revisión se centró en analizar y auditar la documentación asociada a los procesos para identificar oportunidades de mejora y verificar la correcta aplicación de los procedimientos establecidos. Durante la jornada auditora se realiza el análisis y la recopilación de evidencias sobre lo siguiente según sea el caso:

1. Verificar que los manuales de los sistemas contemplen todas las funcionalidades de los aplicativos y que se encuentre disponible para los técnicos y desarrolladores.

2. Verificar que el diseño y construcción del o los aplicativo/s ha sido claramente interpretada por el desarrollista y de acuerdo con los requerimientos del contrato.

3. Verificar que la información básica del sistema con el que se configura para su uso es íntegra, contiene toda la información y ha sido validada por el responsable correspondiente.

4. Verificar que el software ha sido correctamente aprobado y se pueda verificar la versión en producción.

5. Comprobar la estrategia de soporte técnico y los mecanismos de atención previstos para la cobertura de incidencias sean completos y eficientes.

6. Verificar el nivel de conocimiento de los técnicos responsable de soporte para los usuarios de los aplicativos a fin de valorar su capacidad de respuesta durante el uso de los aplicativos.

7. Verificar que los usuarios de los sistemas cuentan con todo el conocimiento y asegurar su capacidad para operar sobre los sistemas.

8. Verificar que el plan de instalación, configuración y puesta en marcha de los equipos a utilizar se ejecuta con una metodología normalizada y segura, garantizando su correcta operación.

9. Verificar que los usuarios de los sistemas cuentan con todo el conocimiento y asegurar su capacidad para operar sobre los sistemas.

### Revisión documental:

La revisión documental se enfocó en los siguientes requerimientos y evidencias solicitadas:

- Documentación técnica del sistema dirigida a los distintos roles, manuales de operación e instructivos de uso y resolución de incidentes.
- Documentación que define y gestiona las características funcionales y no funcionales del sistema (matriz de requerimientos).
- Manuales operativos, instructivos y bitácoras de los procedimientos para la carga de los datos de la elección y autenticación de usuarios.
- Documentación aprobada para la aceptación y liberación del software en producción, así como para la verificación de su autenticidad.
- Registros de incidencias, escalamiento y Acuerdos de Nivel de Servicio (SLA) para soporte técnico.
- Herramientas de consulta, protocolos y autoevaluaciones vinculadas a la capacitación del personal técnico en campo y remoto.
- Disponibilidad de plataformas de consulta, manuales e instructivos para los usuarios finales de los sistemas.
- Otros documentos según sea el caso, como: inventario de equipos, presentaciones de capacitación, actas de entrega.

Pruebas realizadas:

1. Revisión del alcance y amplitud de manuales de sistemas a fin de verificar que los manuales de los sistemas contemplen todas las funcionalidades de los aplicativos y que se encuentre disponible para los técnicos y desarrolladores. Esta revisión tiene como objetivo examinar el soporte documental del sistema para evaluar su funcionamiento y el cumplimiento de los procesos definidos dentro de la organización a fin de comprobar el objetivo de la auditoría. Se busca identificar oportunidades de mejora y verificar la correcta aplicación de los procedimientos establecidos. El enfoque particular es verificar los requerimientos de documentación técnica, manuales de operación,

instructivos de uso, recomendaciones y la disponibilidad de estas herramientas.

Para ello, durante la auditoría, se lleva a cabo la revisión documental de la información suministrada en repositorios compartidos y otros medios de almacenamiento.

El riesgo potencial que motiva la realización de esta verificación es que la ausencia de documentación formal limita la trazabilidad del conocimiento y dificulta la capacitación homogénea de los usuarios. Asimismo, esta situación incrementa la dependencia de prácticas informales o no formalizadas. A largo plazo, reduce la capacidad de demostrar de manera objetiva el alcance funcional, los controles operativos y la madurez del sistema ante futuras revisiones.

2. Revisión de la documentación de características funcionales y no funcionales de los. Su propósito es:

- Evaluar el funcionamiento y el grado de cumplimiento del sistema respecto de los procesos definidos por la organización.
- Contrastar los requerimientos contractuales con la matriz de requerimientos para validar su alcance y completitud.
- Identificar oportunidades de mejora y verificar la correcta aplicación de los procedimientos establecidos.

Para ello, se realiza una revisión documental exhaustiva de los materiales proporcionados por el equipo responsable del sistema, se analiza toda la documentación presentada, se establece la existencia, vigencia y versión de los documentos y se identifica su modalidad de almacenamiento y distribución.

El riesgo potencial que motiva la realización de esta verificación es el riesgo de incumplimiento contractual y asegurar que la fase de desarrollo pueda contemplar adecuadamente las funcionalidades derivadas de los requerimientos.

3. Verificar que la información básica del sistema con el que se configura para su uso es íntegra, contiene toda la información y ha sido validada por el responsable correspondiente. Esta verificación tiene como objetivo evaluar el funcionamiento y cumplimiento de los procesos definidos dentro de la organización en el sistema, así como, identificar oportunidades de mejora y garantizar la correcta aplicación de los procedimientos establecidos.

   Se realiza una revisión documental exhaustiva de los materiales proporcionados por el equipo responsable del sistema, se analiza toda la documentación presentada, se establece la existencia, vigencia y versión de los documentos y se identifica su modalidad de almacenamiento y distribución.

   El riesgo potencial que motiva esta verificación es que la falta de documentación genera riesgos de inconsistencias en la ejecución y dificultades para la capacitación de nuevos recursos. Existe un riesgo de incremento en la dependencia del conocimiento tácito del personal clave, lo cual limita la capacidad de trazabilidad ante incidentes y la demostración formal del cumplimiento de los controles requeridos.

4. Revisión de procedimientos para la aceptación y verificación de autenticidad del software. Su propósito es evaluar los procedimientos tanto para la aceptación de la versión de software que se pondrá en producción como para la verificación de la autenticidad del software a utilizar, además de analizar que la documentación tenga una lectura clara y comprensible.

   Para esta prueba se realiza una revisión documental de los materiales suministrados por el equipo responsable. La revisión se orienta a identificar documentos, registros o soportes relacionados con la aceptación de la versión de software que será puesta en producción. Se busca identificar los mecanismos de verificación de la autenticidad del software a utilizar, se revisan los contenidos independientemente del título o nombre del archivo y se toma como referencia la planilla de

cálculo recibida como respuesta a los requerimientos, y, para mayor certeza se revisan todos los documentos de procesos.

El riesgo potencial que motiva esta verificación es la generación de riesgos operativos, de aseguramiento y de control ante eventuales incidencias o revisiones posteriores y la reducción de la trazabilidad del software puesto en producción y debilitamiento de los mecanismos de control y validación.

5. Evaluar los procedimientos de soporte técnico y mesa de ayuda. Tiene como propósito verificar el cumplimiento sobre los procedimientos de soporte técnico y mesa de ayuda. Asimismo, verificar los procedimientos para el escalamiento de incidencias y consultas, detallando cómo se registran y clasifican según su gravedad y evaluar cómo están establecidos los acuerdos de nivel de servicio (SLA) que determinen tiempos máximos de respuesta y resolución, garantizando la calidad y eficiencia del soporte.

6. Analizar los procedimientos y herramientas de capacitación de los usuarios de los sistemas, su propósito es la verificación de cumplimiento que permita concluir sobre el nivel de conocimiento que adquieren los usuarios en las capacitaciones:

    - Evaluar el funcionamiento y cumplimiento de los procesos de capacitación dirigidos a los usuarios del sistema en cuestión.
    - Confirmar la disponibilidad y correcta actualización de las herramientas de consulta, manuales e instructivos.
    - Garantizar que la documentación entregada corresponda fehacientemente a las versiones vigentes del software y eventos electorales en curso.

Para este análisis, sobre la documentación presentada, se realiza la búsqueda de conceptos que son relevantes al objetivo, de la siguiente forma:

- Ejecución de una revisión documental exhaustiva de los materiales provistos por la organización para la capacitación de usuarios.
- Verificación de la disponibilidad y pertinencia de manuales e instructivos operativos, tanto para los aplicativos instalados en el computador como para el uso de las aplicaciones web (visores).
- Cotejo del contenido de la documentación provista contra las funcionalidades actuales del sistema en producción.
- Análisis de las herramientas o plataformas de consulta de acciones y operaciones destinadas a los usuarios.
- Verificación sobre la existencia de métodos de comprobación de comprensión de los conocimientos recibidos por los usuarios.

### 7.1.3 Seguimiento

La etapa de seguimiento tiene como finalidad verificar la implementación de las medidas correctivas, acciones de mejora y recomendaciones emitidas durante el proceso de auditoría, así como validar la efectividad de los ajustes realizados sobre los sistemas y componentes tecnológicos auditados.

Las actividades de seguimiento se desarrollan de manera continua durante el proceso electoral, permitiendo evaluar la evolución de los hallazgos identificados, la mitigación de riesgos tecnológicos y el fortalecimiento de los controles implementados sobre la infraestructura y los sistemas electorales.

Esta etapa contempla la revisión de evidencias asociadas a correcciones funcionales, ajustes de configuración, fortalecimiento de controles de seguridad, actualización de procedimientos operativos y demás medidas implementadas por las áreas responsables y contratistas vinculados al proceso electoral. El seguimiento constituye un componente fundamental del modelo metodológico, en tanto permite mantener una evaluación continua sobre el estado de situación de los sistemas auditados.

### 7.1.4 Informes

Como parte del desarrollo de la Auditoría Externa Internacional correspondiente al proceso electoral de Presidente y Vicepresidente de la República 2026, los resultados obtenidos durante cada una de las etapas del proceso electoral son consolidados, analizados y documentados de manera independiente, conforme al avance de las actividades de evaluación ejecutadas sobre los sistemas y componentes tecnológicos auditados.

Cada informe incorpora las evidencias técnicas recopiladas, las observaciones derivadas de las actividades de revisión, los hallazgos identificados durante las evaluaciones efectuadas y el estado de situación observado en la etapa correspondiente, permitiendo documentar de manera progresiva la evolución de los sistemas auditados y de los controles implementados sobre la operación tecnológica electoral.

De conformidad con el modelo de ejecución definido para la auditoría presidencial, se contempla la emisión de informes diferenciados para cada etapa del proceso electoral, permitiendo documentar de manera específica las actividades desarrolladas, las evaluaciones realizadas y los resultados obtenidos durante las fases pre-electoral, electoral y post-electoral, según corresponda.

## 7.2 Criterios de Evaluación Técnica

Este apartado desarrolla los mecanismos de valoración técnica aplicados para el análisis de evidencias, evaluación de controles, identificación de riesgos y clasificación de hallazgos sobre los distintos sistemas tecnológicos auditados.

El enfoque metodológico implementado considera principios de evaluación basados en criticidad, impacto potencial, probabilidad de ocurrencia, exposición al riesgo, existencia de controles compensatorios y capacidad

de mitigación, permitiendo determinar de manera razonable el nivel de afectación que una debilidad o vulnerabilidad podría representar sobre la integridad, disponibilidad, confidencialidad, trazabilidad o continuidad operativa de los sistemas electorales.

La valoración técnica contempla igualmente el análisis del contexto operativo de cada sistema auditado, la sensibilidad de la información procesada, el nivel de dependencia funcional del proceso electoral respecto del sistema evaluado y la capacidad institucional para detectar, contener o corregir eventuales incidentes o desviaciones operativas.

### 7.2.1 Identificación de observaciones y hallazgos

Como parte del proceso de auditoría, los resultados obtenidos durante las actividades de revisión documental, validaciones técnicas, pruebas funcionales, verificaciones operativas y evaluaciones de seguridad son clasificados conforme a criterios metodológicos que permiten distinguir entre situaciones que constituyen incumplimientos formales y aquellas que representan oportunidades de mejora o riesgos potenciales.

Con el fin de mantener claridad metodológica en los resultados de la auditoría, se establece la siguiente diferenciación:

#### Observación

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 o afectar la eficiencia del proceso. En estos casos, no se exige necesariamente un plan correctivo inmediato, pero se recomienda su atención preventiva.

#### Hallazgo

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.

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

Asimismo, los hallazgos identificados durante las actividades de auditoría son analizados considerando cuatro elementos fundamentales de evaluación que permiten estructurar técnicamente dichos hallazgos y establecer de manera razonable el nivel de impacto, exposición y riesgo asociado a los sistemas evaluados:

### Condición

Corresponde a la situación identificada durante el proceso de auditoría como resultado de las actividades de revisión documental, validación técnica, análisis de evidencias, pruebas funcionales, evaluaciones de seguridad o verificaciones operativas efectuadas sobre los sistemas auditados. La condición describe el estado observado del control, proceso, configuración, sistema o procedimiento evaluado, constituyendo el hecho objetivo evidenciado por el equipo auditor durante el desarrollo de las actividades técnicas. La condición responde a ¿Qué se encontró?

### Criterio

Corresponde al marco de referencia utilizado para evaluar la condición identificada y determinar si existe o no desviación respecto de los parámetros esperados de cumplimiento, control o funcionamiento. El criterio puede derivarse de disposiciones contractuales, requerimientos funcionales, documentación técnica, lineamientos institucionales, estándares internacionales, buenas prácticas de seguridad, procedimientos operativos, arquitecturas definidas, controles establecidos o marcos metodológicos aplicables al proceso electoral y a los sistemas auditados.

### Causa

Corresponde al origen o factor que genera la condición observada y explica la existencia de la desviación, debilidad, vulnerabilidad o incumplimiento identificado durante la auditoría. El análisis de causa permite determinar los factores técnicos, operativos, procedimentales, organizacionales o de control que contribuyeron a la materialización de la condición observada, facilitando la identificación de acciones correctivas y oportunidades de mejora orientadas a mitigar riesgos y fortalecer los controles existentes. La casusa responde a ¿Por qué ocurrió la situación detectada?

### Efecto / Riesgo

Corresponde a la consecuencia real o potencial que la situación detectada podría generar sobre la integridad, confiabilidad, eficiencia o seguridad del proceso auditado. El efecto permite dimensionar el nivel de exposición al riesgo y la eventual afectación que podría generarse sobre la operación electoral, la calidad de la información procesada o la estabilidad de los servicios tecnológicos. Permite priorizar el hallazgo y orientar la toma de decisiones respecto a su tratamiento.

## 7.2.2 Clasificación de Hallazgos

Los hallazgos identificados durante el desarrollo de la auditoría son clasificados conforme a tres niveles de criticidad:

- Alto (Riesgo Crítico): Podría comprometer directamente la integridad del proceso electoral, la confidencialidad del voto o generar fallas graves. Requiere atención inmediata y acción correctiva prioritaria.
- Medio (Riesgo Relevante): Puede afectar parcialmente el proceso o la información, pero no amenaza la operación general. Debe corregirse de manera planificada.
- Bajo (Riesgo Menor): Impacto limitado o poco probable. Se recomienda monitoreo o mejora en procesos de soporte.

# VIII. RESULTADOS DE LA AUDITORÍA

Los resultados expuestos en este capítulo corresponden a las actividades de evaluación ejecutadas sobre los sistemas de información, componentes tecnológicos e infraestructura incluidos dentro del alcance de la Auditoría de Sistemas para la fase pre-electoral. Las verificaciones efectuadas permitieron obtener evidencia técnica independiente respecto de las condiciones de funcionamiento, seguridad, integridad, disponibilidad y soporte operativo de los componentes auditados, así como de su grado de cumplimiento frente a los requerimientos establecidos para el proceso electoral.

El análisis desarrollado proporciona una valoración técnica sobre el estado de los sistemas y recursos tecnológicos evaluados durante el período auditado, sustentada en las pruebas realizadas, la revisión documental, el análisis de configuraciones, las validaciones funcionales, análisis de código fuente y las demás actividades contempladas en el plan de auditoría. Las conclusiones y resultados presentados reflejan exclusivamente las condiciones observadas dentro de la delimitación temporal y el alcance definido para esta etapa, sin extenderse a componentes, períodos o escenarios no comprendidos en las actividades de evaluación ejecutadas.

## 8.1 Sistema de Sorteo de Jurados de Votación

La evaluación de este componente tuvo como propósito verificar la capacidad del Sistema de Jurados de Votación para soportar de forma segura y controlada los procesos de conformación, selección, designación y administración de jurados, así como validar la existencia de mecanismos técnicos, operativos y metodológicos orientados a garantizar la trazabilidad, estabilidad, seguridad y calidad del software utilizado durante el proceso electoral.

Los análisis efectuados permitieron evidenciar una solución tecnológica desarrollada bajo una arquitectura basada en microservicios soportada sobre infraestructura en la nube, complementada con mecanismos de alta

disponibilidad, balanceo de carga y resiliencia operativa. Asimismo, se constató la utilización de motores PostgreSQL y Amazon Aurora PostgreSQL para la gestión de la información, junto con mecanismos de persistencia mediante consultas parametrizadas que contribuyen a preservar la integridad y seguridad de los datos procesados por el sistema.

La revisión del código fuente permitió verificar el adecuado funcionamiento de los procesos asociados a la carga de información, parametrización de criterios, ejecución del sorteo, conformación de mesas y generación de reportes, evidenciándose correspondencia entre las funcionalidades implementadas y las reglas de operación definidas para el componente. De igual forma, se observó la aplicación de metodologías formales de desarrollo, control de cambios y versionamiento soportadas mediante Scrum, Azure DevOps y GitFlow, proporcionando mecanismos adecuados de organización, seguimiento y trazabilidad durante el ciclo de vida del software.

La auditoría también se enfocó en validar los mecanismos de seguridad implementados sobre la solución. En este sentido, se evidenció la ejecución de pruebas unitarias, funcionales y de integración, así como análisis estático de código fuente, cuyos resultados no identificaron vulnerabilidades confirmadas de severidad alta o crítica. Adicionalmente, se generó la línea base de integridad mediante valores hash SHA-256 para su posterior verificación respecto de las versiones destinadas a producción.

Desde la perspectiva operativa, se verificó la existencia de mecanismos para la gestión y trazabilidad de requerimientos, observándose alineación entre las funcionalidades desarrolladas y los requerimientos definidos para el componente. Asimismo, las actividades de validación realizadas permitieron evidenciar un adecuado conocimiento funcional de los procesos asociados al sistema por parte del personal involucrado, identificándose oportunidades de fortalecimiento relacionadas con la formalización documental.

En consecuencia, y dentro de los límites metodológicos y de alcance definidos para la presente fase de auditoría, el sistema presenta condiciones técnicas que permiten sustentar una conclusión favorable respecto de su estabilidad operativa, trazabilidad, seguridad, control de desarrollo y conformidad funcional para la etapa evaluada.

Con base en las evidencias técnicas revisadas, incluyendo documentación metodológica, análisis de código fuente, validaciones funcionales, revisión de la arquitectura tecnológica y análisis estático de seguridad, no se identificaron hallazgos críticos, vulnerabilidades ni observaciones que comprometan la estabilidad, seguridad, integridad o funcionamiento del sistema. En consecuencia, se concluye que el Sistema de Jurados 2026 presenta un adecuado nivel de madurez técnica, control operativo, trazabilidad y conformidad funcional, evidenciando condiciones favorables para su operación dentro de un entorno electoral de alta disponibilidad.

### Resumen de resultados


## 8.2 Sistema de Preconteo y Comunicaciones

La evaluación de este componente tuvo como propósito verificar la capacidad del Sistema de Preconteo para soportar de forma segura, estable y controlada los procesos de recepción, procesamiento, consolidación y publicación de resultados electorales preliminares, así como validar la existencia de mecanismos técnicos, operativos y metodológicos orientados a garantizar la disponibilidad, trazabilidad,

seguridad e integridad de la información procesada durante la jornada electoral.

Los análisis efectuados permitieron evidenciar una solución tecnológica de misión crítica soportada sobre una arquitectura híbrida que integra componentes locales y servicios desplegados en la nube, diseñada para atender requerimientos de alta disponibilidad, procesamiento distribuido y continuidad operativa. Asimismo, se constató la utilización de mecanismos de balanceo de carga, distribución de servicios, redundancia y resiliencia operativa, complementados con motores de base de datos utilizados para la gestión de la información y el procesamiento de los resultados electorales preliminares.

La revisión del código fuente y las actividades de depuración realizadas permitieron verificar el adecuado funcionamiento de los procesos asociados a la digitalización de formularios electorales, reconocimiento óptico de información, consolidación de resultados, monitoreo operativo, generación de archivos y emisión de reportes y boletines oficiales. De igual forma, se evidenció correspondencia entre las funcionalidades implementadas y las reglas de operación definidas para el componente, así como la correcta ejecución de los procesos observados durante las validaciones efectuadas.

La auditoría también se enfocó en validar los mecanismos de desarrollo, control de cambios y versionamiento implementados sobre la solución. En este sentido, se observó la utilización de metodologías ágiles para la gestión de requerimientos y seguimiento de actividades, así como herramientas especializadas para el control de versiones, trazabilidad y administración del ciclo de vida del software. Asimismo, se verificó la ejecución de pruebas funcionales, pruebas de integración y análisis estático y dinámico de código orientados a la identificación temprana de errores, vulnerabilidades y desviaciones técnicas antes de su despliegue a producción.

Desde la perspectiva de seguridad, se constató la existencia de mecanismos de autenticación centralizada, controles perimetrales, registros de auditoría, trazabilidad operativa y controles orientados a la protección de la información procesada por el sistema. Las evaluaciones de seguridad realizadas permitieron identificar oportunidades de mejora sobre algunos componentes tecnológicos, respecto de las cuales se verificó la existencia de medidas de mitigación y controles compensatorios orientados a reducir el riesgo residual asociado.

Desde la perspectiva operativa, se verificó la existencia de controles operativos, documentación funcional, matrices de requerimientos alineadas con las necesidades del componente, herramientas de capacitación y personal técnico con conocimiento suficiente sobre las plataformas evaluadas, lo que permitió el adecuado desarrollo de las actividades observadas durante las pruebas y validaciones realizadas identificándose oportunidades de fortalecimiento documental de procedimientos técnicos, operativos y de contingencia.

En consecuencia, y dentro de los límites metodológicos y de alcance definidos para la presente fase de auditoría, el componente presenta condiciones técnicas que permiten sustentar una conclusión favorable respecto de su estabilidad operativa, trazabilidad, disponibilidad, seguridad y conformidad funcional para la etapa evaluada.

Con base en las evidencias técnicas revisadas, incluyendo análisis de código fuente, actividades de depuración, validaciones funcionales, revisión de la arquitectura tecnológica, evaluaciones de seguridad y verificaciones operativas, no se identificaron hallazgos con riesgos residuales que comprometan la estabilidad, disponibilidad o funcionamiento general del sistema auditado ni condiciones que pudiesen afectar la integridad del proceso electoral. Los hallazgos identificados durante las actividades de evaluación cuentan con controles y medidas de mitigación que mantienen un nivel de riesgo residual bajo. Por tanto, se concluye que el Sistema de Preconteo presenta un adecuado nivel de madurez tecnológica y operativa, evidenciándose condiciones favorables

de estabilidad, trazabilidad, disponibilidad y conformidad funcional para soportar el procesamiento y publicación de resultados electorales preliminares en un entorno de alta criticidad.

Resumen de resultados


## 8.3 Sistema para la realización de Escrutinios

La evaluación de este componente tuvo como propósito verificar la capacidad del Sistema de Escrutinio para soportar de forma segura, estable y controlada los procesos de recepción, consolidación, validación y consulta de resultados electorales, así como validar la existencia de mecanismos técnicos, operativos y metodológicos orientados a garantizar la disponibilidad, trazabilidad, integridad y seguridad de la información procesada durante el proceso electoral.

Los análisis efectuados permitieron evidenciar una solución tecnológica soportada sobre infraestructura en la nube, diseñada bajo una arquitectura que incorpora mecanismos de balanceo de carga, procesamiento concurrente, distribución de servicios y resiliencia operativa para atender los requerimientos de disponibilidad y desempeño propios de un sistema electoral de alta criticidad. Asimismo, se constató la utilización de componentes para la recepción, consolidación, almacenamiento y consulta de resultados electorales, así como mecanismos orientados a preservar la integridad de la información generada por el sistema.

La revisión del código fuente y las actividades de depuración realizadas permitieron verificar el adecuado funcionamiento de los procesos asociados a la digitalización de formularios E-14, recepción y consolidación de información electoral, validaciones, monitoreo operativo, generación de archivos y emisión de reportes y publicaciones vinculadas al proceso electoral. De igual forma, se evidenció correspondencia entre las funcionalidades implementadas y las reglas de operación definidas para el componente, así como la correcta ejecución de los procesos observados durante las validaciones efectuadas.

Sobre la validación de los mecanismos de desarrollo, control de cambios y versionamiento se observó la utilización de metodologías ágiles para la gestión de requerimientos, trazabilidad y seguimiento de actividades, así como procedimientos formales para la aprobación, validación y despliegue controlado de nuevas funcionalidades. Asimismo, se verificó la ejecución de pruebas funcionales, pruebas de integración y análisis de código orientados a la identificación preventiva de vulnerabilidades, errores y desviaciones técnicas durante el ciclo de desarrollo.

Desde la perspectiva de seguridad, se evaluaron los controles implementados sobre el software y los equipos utilizados para la operación del sistema, incluyendo análisis estático de código fuente, análisis dinámico mediante depuración e inspección de tráfico, validaciones de hardening y revisión del procedimiento de enrolamiento de equipos. Las pruebas realizadas permitieron evidenciar la efectividad de los controles de restricción de ejecución de software no autorizado, estos controles mostraron un funcionamiento efectivo que impidió ejecutar aplicaciones fuera de la línea base autorizada, acceder a la línea de comandos o modificar configuraciones críticas del sistema operativo durante las pruebas efectuadas. Asimismo, se verificó que el procedimiento de enrolamiento incorpora controles técnicos y procedimentales orientados a validar la incorporación de equipos a la operación electoral. Como resultado de las actividades realizadas, no se identificaron hallazgos críticos de seguridad que comprometieran el funcionamiento del componente dentro del alcance evaluado.

Desde la perspectiva operativa, se evidenció un adecuado desempeño del sistema durante las pruebas y simulacros realizados, respaldado por el conocimiento funcional y técnico del personal involucrado en la operación de la solución. Asimismo, se verificó la existencia de mecanismos de gestión y seguimiento que permiten soportar la ejecución de las actividades asociadas al componente identificándose como oportunidad de mejora el fortalecimiento documental.

En consecuencia, y dentro de los límites metodológicos y de alcance definidos para la presente fase de auditoría, el componente presenta condiciones técnicas que permiten sustentar una conclusión favorable respecto de su estabilidad operativa, trazabilidad, disponibilidad, seguridad y conformidad funcional para la etapa evaluada.

Como resultado de las revisiones, pruebas y validaciones efectuadas, no se identificaron hallazgos críticos que comprometan la estabilidad, seguridad, disponibilidad o funcionamiento general del sistema que pudiesen afectar la integridad del proceso electoral. En consecuencia, se concluye que el Sistema de Escrutinio presenta un adecuado nivel de madurez técnica, control operativo, trazabilidad y conformidad funcional para soportar las operaciones electorales en un entorno de alta criticidad.

## Resumen de resultados

## 8.4 Sistema de Consolidación y Divulgación de Resultados Electorales

La evaluación de este componente tuvo como propósito verificar la capacidad del Sistema de Consolidación y Divulgación de Resultados para soportar de forma segura, estable y controlada los procesos de recepción, procesamiento, consolidación y publicación de información electoral, así como validar la existencia de mecanismos técnicos, operativos y metodológicos orientados a garantizar la disponibilidad, integridad, trazabilidad y confiabilidad de la información divulgada durante el proceso electoral.

Los análisis efectuados permitieron evidenciar una plataforma tecnológica diseñada para el procesamiento y publicación de información electoral en tiempo real, soportada sobre una arquitectura orientada a la alta disponibilidad, escalabilidad, desacoplamiento funcional y tolerancia a fallos. Asimismo, se constató la existencia de componentes especializados para la validación, procesamiento y divulgación de información electoral, permitiendo la ejecución concurrente de tareas de consolidación y la generación de productos de información destinados a diferentes canales de publicación.

La revisión del código fuente y las actividades de depuración realizadas permitieron verificar el adecuado funcionamiento de los procesos asociados a la recepción, validación, procesamiento y consolidación de información proveniente de los sistemas electorales relacionados, así como la generación de archivos y productos de divulgación utilizados para la publicación de resultados. De igual forma, se evidenció correspondencia entre las funcionalidades implementadas y las reglas de operación definidas para el componente, así como la correcta ejecución de los procesos observados durante las validaciones efectuadas.

En la revisión de los mecanismos de desarrollo, control de cambios y versionamiento de software se verificó la existencia de procedimientos

formales para la gestión de cambios, trazabilidad y control de versiones, así como la ejecución de pruebas unitarias, funcionales e integrales y análisis estático de código orientados a la identificación preventiva de vulnerabilidades, errores lógicos y desviaciones técnicas durante el ciclo de desarrollo.

En materia de seguridad, se realizaron análisis estático y dinámico sobre el software bajo modalidad de caja gris, permitiendo evaluar controles de autenticación y autorización sobre los principales flujos funcionales del sistema. Las pruebas efectuadas permitieron evidenciar la efectividad de los controles de acceso implementados, sin que fuera posible eludir las restricciones asociadas al perfil utilizado durante las validaciones. Asimismo, el análisis de código fuente no identificó vulnerabilidades de severidad crítica o alta dentro del alcance evaluado.

Desde la perspectiva operativa, la operación observada durante simulacros y pruebas mostró un desempeño estable y eficiente, sustentado en la experiencia y conocimiento práctico del personal técnico involucrado en el proceso. Asimismo, las actividades de auditoría permitieron identificar oportunidades de mejora relacionadas con la formalización documental operativa.

En consecuencia, y dentro de los límites metodológicos y de alcance definidos para la presente fase de auditoría, el componente presenta condiciones técnicas que permiten sustentar una conclusión favorable respecto de su estabilidad operativa, escalabilidad, integridad, seguridad y conformidad funcional para la etapa evaluada.

Los resultados obtenidos evidenciaron que no se identificaron hallazgos críticos, fallas de lógica, debilidades de implementación ni observaciones que comprometan la estabilidad, seguridad, disponibilidad o funcionamiento general del sistema que pudiesen afectar la integridad del proceso electoral.

Con fundamento en los resultados obtenidos, se concluye que el Sistema de Consolidación y Divulgación de Resultados presenta un nivel satisfactorio de seguridad y un alto nivel de madurez tecnológica, con condiciones favorables de estabilidad, escalabilidad, integridad y confiabilidad para soportar procesos electorales de alta criticidad y exposición pública.

Resumen de resultados


## 8.5 Infraestructura tecnológica

La evaluación de este componente tuvo como propósito verificar la capacidad de la infraestructura tecnológica y los mecanismos de ciberseguridad implementados para soportar de forma segura, estable y continua la operación de los sistemas electorales auditados, así como validar la existencia de controles orientados a garantizar la disponibilidad, redundancia, escalabilidad, monitoreo y protección de los activos tecnológicos que soportan el proceso electoral.

Las actividades de auditoría comprendieron la revisión documental de los componentes de infraestructura y ciberseguridad, sesiones técnicas con el personal responsable de su administración, validación de configuraciones, revisión de diagramas de arquitectura y topologías, análisis de procedimientos operativos y visitas técnicas a los centros de datos utilizados para la operación de los sistemas electorales. Como resultado de estas verificaciones, se evidenció la existencia de un modelo integral de infraestructura tecnológica y ciberseguridad diseñado para soportar las

necesidades operativas y de disponibilidad requeridas para el proceso electoral.

Los análisis efectuados permitieron constatar la existencia de componentes de alta disponibilidad, esquemas de redundancia continua y mecanismos de escalabilidad implementados sobre las plataformas tecnológicas auditadas. Asimismo, durante las visitas realizadas a los centros de datos se verificó el cumplimiento de las certificaciones internacionales requeridas contractualmente, así como la disponibilidad de capacidades físicas y tecnológicas orientadas a garantizar la continuidad operativa de los servicios soportados.

Se verificó la existencia de documentación operativa y técnica asociada a la administración de la infraestructura, incluyendo inventarios de hardware y software, diagramas de arquitectura lógica y física, matrices de dimensionamiento, procedimientos de respaldo y recuperación, gestión de cambios, administración de accesos, retención de registros y monitoreo de eventos. Asimismo, se evidenció la implementación de controles y herramientas de seguridad orientadas a la protección de los componentes tecnológicos desplegados para el proceso electoral.

Desde la perspectiva de ciberseguridad, se constató la implementación de un esquema de protección basado en múltiples capas de seguridad, complementado con capacidades de monitoreo permanente mediante un Security Operation Center (SOC) que opera de forma coordinada con el SOC de la Registraduría Nacional, permitiendo la vigilancia continua de eventos, amenazas y riesgos asociados a la operación electoral. De igual forma, se verificó que los procesos de hardening implementados cumplen con los lineamientos y estándares definidos para este propósito.

En consecuencia, y dentro de los límites metodológicos y de alcance definidos para la presente fase de auditoría, el componente presenta condiciones técnicas que permiten sustentar una conclusión favorable respecto de su disponibilidad, redundancia, capacidad operativa y seguridad para la operación de los sistemas electorales evaluados.

Durante las actividades de revisión y pruebas efectuadas no se evidenciaron situaciones que permitan prever afectaciones sobre la continuidad, disponibilidad o funcionamiento general del componente evaluado. Se verificó que las implementaciones de infraestructura cumplen con las capacidades operativas requeridas para los componentes auditados, sin menoscabo de la seguridad de la información, la funcionalidad, la operatividad, la continuidad del servicio ni los mecanismos de alta disponibilidad exigidos para la operación electoral.

En consecuencia, se concluye que las plataformas implementadas para los componentes auditados cuentan con un modelo de infraestructura tecnológica y ciberseguridad integral y robusto para la operación y desarrollo de los componentes electorales de la elección de Presidente y Vicepresidente de la República.

Resumen de resultados

# IX. VERSIONAMIENTO Y CUSTODIA DE SOFTWARE

En el marco del proceso electoral para la elección de Presidente y Vicepresidente de la República, la Registraduría Nacional del Estado Civil (RNEC) y las firmas contratistas ejecutan de forma obligatoria y ordinaria el procedimiento de sellado y puesta en custodia de las soluciones tecnológicas que operarán en la jornada electoral. El rol fundamental de este equipo auditor consistió en realizar una verificación técnica independiente de dicho proceso. Esto se hizo con el fin de verificar que el software sellado y puesto en custodia correspondiera con las versiones de software exactas que fueron revisadas y validadas por la auditoría.

Para cumplir con este objetivo de control, la metodología de la auditoría se basó en el cotejo criptográfico. Durante las etapas previas de revisión de código fuente y pruebas funcionales, el equipo auditor generó de manera independiente valores únicos de verificación (hashes) sobre los archivos definitivos de cada software. Estas huellas digitales inalterables sirvieron como el estándar de comparación técnica indispensable para corroborar la identidad y la inmutabilidad del software durante los eventos oficiales de sellado.

En ese sentido, la auditoría realizó el acompañamiento y la verificación de la identidad del software el 28 de mayo de 2026, participando en dos sesiones programadas para el procedimiento de sellado y custodia

En la primera sesión realizada a las 9h00, de la mañana en las instalaciones ubicadas en la Calle 26 #102-21, Oficina 613, Buró 26, se presenció el procedimiento de sellado y puesta en custodia de las versiones de software destinadas a los sistemas de Preconteo y Escrutinio. Al finalizar el acto, la auditoría corroboró mediante el análisis de firmas (hash) que la versión de software resguardada corresponde de forma inequívoca a la misma versión previamente auditada.

Posteriormente, en la jornada de la tarde, a las 2:30 pm en las instalaciones ubicadas en Bogotá calle 93 #16-25- Sala de Centro de Gestión Nacional, se acompañó el proceso de sellado y custodia del software de Consolidación y Divulgación de resultados, donde el equipo auditor verificó y comprobó que los archivos protegidos coincidían plenamente con las versiones revisadas y validadas en el proceso de auditoría.

A partir de los cotejos y validaciones criptográficas ejecutadas en las jornadas descritas, se constató una coincidencia absoluta entre los valores hash del software sellado y los componentes evaluados a lo largo del proceso de auditoría.

En consecuencia, se emite un criterio técnico de verificación favorable en el que se establece que las versiones de software de escrutinio, preconteo, consolidación y divulgación entregadas en custodia el día 28 de mayo de 2026, corresponden estrictamente con las versiones de software sobre las cuales esta auditoría ha emitido criterio técnico en este informe

# X. CONCLUSIONES

Con fundamento en la evidencia técnica y documental obtenida durante el desarrollo de la Auditoría de Sistemas, y dentro del alcance definido en el marco contractual aplicable, los sistemas de información, procesos e infraestructura tecnológica auditados presentan un nivel adecuado de cumplimiento respecto de los requerimientos funcionales, técnicos, operativos y de seguridad establecidos para la fase pre-electoral del proceso de elección de Presidente y Vicepresidente de la República.

Las actividades de evaluación realizadas sobre los sistemas de Jurados de Votación, Preconteo, Escrutinio, Consolidación y Divulgación de Resultados e Infraestructura Tecnológica permitieron verificar la existencia de mecanismos formales de desarrollo, control de cambios, versionamiento de software, trazabilidad, monitoreo, seguridad, alta disponibilidad, redundancia y continuidad operativa, evidenciándose condiciones consistentes con las necesidades de operación de un proceso electoral de alta criticidad.

De manera general, los resultados obtenidos evidenciaron que no se mantienen hallazgos con riesgos residuales que comprometan la estabilidad, disponibilidad, seguridad, integridad o funcionamiento de los componentes evaluados.

Las revisiones funcionales, técnicas y de seguridad efectuadas sobre los componentes auditados permitieron evidenciar un comportamiento consistente con los requerimientos definidos para la etapa evaluada. Asimismo, las validaciones realizadas sobre la infraestructura tecnológica y los componentes de ciberseguridad permitieron constatar la existencia de mecanismos de protección, monitoreo y resiliencia orientados a preservar la continuidad de los servicios que soportan la operación electoral.

En relación con la integridad y trazabilidad del software electoral, el equipo auditor realizó la verificación técnica independiente y el cotejo criptográfico de los valores hash generados durante las actividades de auditoría, constatando que las versiones de software selladas y puestas en custodia por la Registraduría Nacional del Estado Civil corresponden íntegramente con el software de Preconteo, Escrutinio, Consolidación y Divulgación previamente evaluado en esta auditoría.

Las conclusiones expuestas se emiten dentro de los límites metodológicos, temporales y de alcance definidos para la presente fase de auditoría y con fundamento en las evidencias obtenidas durante el ejercicio de verificación independiente, por tanto, no constituyen una garantía de comportamiento futuro en condiciones distintas a las evaluadas.

En consecuencia, y para la fase pre-electoral evaluada, se emite un concepto técnico favorable respecto de los sistemas de información, procesos e infraestructura tecnológica auditados, considerando que los componentes evaluados disponen de controles y mecanismos razonablemente adecuados para soportar de forma segura, estable y continua la operación de la elección de Presidente y Vicepresidente de la República.

Dado que el proceso electoral continúa su ejecución en las fases electoral y post electoral previstas dentro del alcance contractual, las actividades de auditoría continuarán desarrollándose conforme a la planificación establecida para las siguientes etapas.

IIDH / CAPEL