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
SEGUNDA VUELTA
JORNADA ELECTORAL

24 de junio, 2026

Elección Presidencial

INFORME 2da VUELTA JORNADA ELECTORAL

Elección Presidencial

CONTENIDO

I. INTRODUCCIÓN

En cumplimiento de las actividades de Auditoría Externa Internacional de Sistemas para la elección de Presidente y Vicepresidente de la República de Colombia 2026, el Instituto Interamericano de Derechos Humanos, a través del Centro de Asesoría y Promoción Electoral (IIDH/CAPEL), desarrolló las actividades de auditoría correspondientes a la fase electoral de la segunda vuelta presidencial, orientadas a verificar el comportamiento operativo, funcional y de seguridad de los sistemas de información, procesos e infraestructura tecnológica que soportaron la organización, ejecución y divulgación de los resultados del proceso electoral.

La fase electoral constituye el momento de mayor criticidad dentro del ciclo de auditoría, por cuanto permite observar el funcionamiento de los sistemas en condiciones reales de operación, validar la efectividad de los controles previamente evaluados durante las etapas preparatorias y verificar la capacidad de los diferentes componentes tecnológicos para responder de manera continua, segura y confiable ante las exigencias propias de una jornada electoral.

Las actividades desarrolladas comprendieron el seguimiento técnico de los sistemas electorales, el monitoreo de la infraestructura tecnológica y de ciberseguridad, la observación de los procesos de transmisión, procesamiento, consolidación y divulgación de resultados, así como la atención y análisis de eventos operativos e incidentes reportados durante las distintas etapas de la jornada electoral. De igual forma, se efectuaron verificaciones sobre la integridad de las versiones de software utilizadas en producción, con el propósito de constatar su correspondencia con las versiones previamente auditadas y autorizadas para su utilización durante el proceso electoral.

La ejecución de la auditoría se realizó mediante la aplicación de procedimientos técnicos de observación, revisión documental, análisis de evidencias, seguimiento operativo y verificación de controles, desarrollados directamente en los centros de operación, monitoreo y procesamiento

habilitados para soportar la elección presidencial. Estas actividades permitieron obtener evidencia suficiente y apropiada sobre el desempeño de los componentes auditados, así como sobre la efectividad de los mecanismos de seguridad, disponibilidad, continuidad operativa y gestión de incidentes implementados para la protección de la plataforma tecnológica electoral.

El presente informe expone los resultados obtenidos durante la jornada electoral de la segunda vuelta presidencial, incorporando las principales actividades ejecutadas, las verificaciones realizadas por el equipo auditor, los hallazgos y observaciones identificados, así como las conclusiones derivadas de la evidencia recopilada. Su contenido proporciona una valoración técnica independiente sobre el comportamiento de los sistemas e infraestructura tecnológica durante la operación electoral y sobre el nivel de cumplimiento observado respecto de los requerimientos funcionales, operativos y de seguridad establecidos para el proceso electoral.

II. OBJETIVOS DE LA AUDITORÍA

2.1 Objetivo General

Verificar las condiciones de operación, disponibilidad, integridad y seguridad de los componentes tecnológicos que soportaron la segunda vuelta de la elección de Presidente y Vicepresidente de la República de Colombia 2026, mediante actividades de observación, monitoreo y validación técnica desarrolladas durante la elección.

2.2 Objetivos específicos

1. Verificar las condiciones de disponibilidad y continuidad operativa de la infraestructura tecnológica y de los servicios que soportaron la operación electoral.
2. Observar el comportamiento de las plataformas utilizadas para el procesamiento, consolidación, escrutinio y divulgación de resultados electorales durante su operación en ambiente productivo.
3. Dar seguimiento a los mecanismos de monitoreo y protección implementados para la gestión de eventos de seguridad y la preservación de la estabilidad de los servicios tecnológicos.
4. Validar la integridad de las versiones de software utilizadas durante la jornada electoral mediante la verificación de los mecanismos de control implementados para su resguardo y utilización en producción.
5. Analizar los eventos e incidentes relevantes registrados durante el período evaluado y valorar su incidencia sobre la operación de los servicios incluidos dentro del alcance de auditoría.
6. Obtener evidencia técnica suficiente que permita emitir una valoración independiente sobre las condiciones observadas durante la operación de los componentes tecnológicos que soportaron el proceso electoral.

III. ALCANCE DE LA AUDITORÍA DE SISTEMAS

La auditoría comprende las actividades de verificación técnica efectuadas sobre los sistemas de información, la infraestructura tecnológica y los mecanismos de seguridad que soportaron la segunda vuelta de la elección de Presidente y Vicepresidente de la República de Colombia 2026.

Las actividades desarrolladas se orientaron a verificar las condiciones de disponibilidad, continuidad operativa, capacidad de procesamiento y protección de los servicios tecnológicos involucrados en el procesamiento, consolidación, escrutinio y divulgación de resultados electorales, así como el comportamiento observado de dichos componentes durante su operación en ambiente productivo.

Asimismo, el alcance contempla la validación de la integridad de las versiones de software utilizadas en los sistemas de Preconteo, Escrutinio y Consolidación y Divulgación de Resultados, mediante la revisión de las evidencias técnicas y la aplicación de procedimientos de verificación criptográfica.

Se consideró además el análisis de los eventos de seguridad, incidentes operativos, indicadores de desempeño, mecanismos de protección tecnológica y demás elementos asociados a la operación de los componentes incluidos dentro del alcance de auditoría.

Las actividades desarrolladas se ejecutan dentro de los límites establecidos en el Anexo Técnico y demás instrumentos contractuales que regulan el alcance de la Auditoría Internacional de Sistemas.

IV. DELIMITACIÓN TEMPORAL DEL ENCARGO

La ejecución de las actividades objeto del presente informe se desarrolló durante los días 20 y 21 de junio de 2026, en el marco de la segunda vuelta de la elección presidencial 2026. El período evaluado comprende las verificaciones efectuadas sobre los componentes tecnológicos previo al inicio de la jornada electoral, así como las actividades de observación y seguimiento realizadas durante las fases de votación, transmisión, procesamiento, consolidación y divulgación de resultados preliminares, incluyendo el inicio de las actividades de escrutinio.

Asimismo, dentro de este intervalo se efectuó la recopilación y análisis de las evidencias técnicas, registros operativos e información generada por los diferentes componentes tecnológicos incluidos dentro del alcance de auditoría, con el propósito de valorar las condiciones observadas durante su operación.

Por consiguiente, los resultados, observaciones y conclusiones presentados en este informe se encuentran limitados a los hechos y condiciones verificadas durante el período señalado y dentro del alcance definido para la fase electoral de la Auditoría Internacional de Sistemas.

V. MARCO NORMATIVO Y TÉCNICO

La valoración técnica efectuada se sustentó en los instrumentos contractuales que regulan la Auditoría Externa Internacional de Sistemas, así como en estándares y buenas prácticas ampliamente reconocidos para la auditoría de tecnologías de información, la gestión de infraestructura tecnológica, la seguridad de la información y la continuidad operativa.

Los criterios de evaluación aplicados se fundamentan principalmente en los Contratos 049 y 060 de 2025, sus anexos técnicos y la documentación complementaria que define el alcance, los objetivos y las condiciones bajo las cuales se desarrolla la auditoría de los componentes tecnológicos que soportan el proceso electoral.

Como referencia metodológica se consideraron los lineamientos establecidos por ISACA para auditoría de sistemas de información, los principios de gobierno y control de tecnologías de información contenidos en COBIT, las directrices para auditoría definidas por la norma ISO 19011 y las buenas prácticas relacionadas con la gestión de riesgos, la seguridad de la información, la resiliencia tecnológica y la continuidad de los servicios.

De igual manera, se tomaron en consideración los procedimientos operativos, controles de seguridad, mecanismos de protección tecnológica y esquemas de continuidad implementados para la operación electoral, en tanto constituyen elementos relevantes para la valoración de las condiciones observadas durante el período evaluado.

La aplicación conjunta de estos referentes proporcionó el marco de análisis utilizado para interpretar la evidencia recopilada, valorar los resultados obtenidos y sustentar las conclusiones técnicas presentadas en este informe.

VI. METODOLOGÍA DE AUDITORÍA

Las actividades desarrolladas se orientaron a la obtención y análisis de evidencia técnica sobre la integridad de los sistemas de información, la operación de la infraestructura tecnológica y la efectividad de los mecanismos implementados para la protección de los servicios que soportaron el proceso electoral.

La auditoría fue ejecutada bajo un enfoque basado en riesgos, priorizando aquellos componentes cuya afectación podría incidir sobre la disponibilidad, integridad, continuidad operativa o seguridad de los servicios tecnológicos asociados al procesamiento, escrutinio, consolidación y divulgación de resultados electorales.

Se efectuó la validación criptográfica de las versiones de software utilizadas en los sistemas de Preconteo, Escrutinio y Consolidación y Divulgación de Resultados, ejecutando controles técnicos al inicio y cierre de la jornada electoral, con el propósito de verificar la integridad y correspondencia de las versiones de software con respecto a los componentes puestos en operación para atender la elección.

Se analizaron las condiciones de operación de la infraestructura tecnológica, los mecanismos de continuidad operativa y los controles de seguridad implementados para la protección de los servicios electorales, mediante la revisión de registros operativos, indicadores de desempeño, reportes técnicos y demás evidencias generadas durante el período evaluado.

Asimismo, se consideró la información proveniente de los mecanismos de monitoreo y gestión de ciberseguridad implementados para la jornada electoral, incluyendo eventos de seguridad, incidentes operativos, actividades de protección perimetral, vigilancia de amenazas y acciones de respuesta desarrolladas por los equipos responsables de la operación tecnológica.

VII. RESULTADOS DE LA AUDITORÍA

Los resultados expuestos en este apartado corresponden a las verificaciones realizadas, las cuales estuvieron orientadas a validar la integridad de los sistemas de información utilizados durante la jornada electoral, analizar el comportamiento de la infraestructura tecnológica que soportó la operación electoral y valorar la efectividad de los mecanismos implementados para la protección de los servicios y la gestión de eventos de ciberseguridad.

La información analizada proviene de las evidencias técnicas recopiladas por el equipo auditor sobre los registros generados durante la operación de los sistemas electorales, los reportes de infraestructura y seguridad de los centros de operaciones de seguridad (SOC), así como de las actividades de verificación ejecutadas directamente sobre los componentes incluidos dentro del alcance de auditoría.

De conformidad con las principales áreas de evaluación desarrolladas durante esta etapa, se presentan los resultados de forma agrupada, permitiendo exponer las condiciones observadas respecto de la integridad de los sistemas, la operación de la infraestructura tecnológica y la protección de los servicios que soportaron el proceso electoral.

7.1 Integridad de los sistemas electorales

La verificación de la integridad de los sistemas electorales constituyó una de las actividades desarrolladas durante la fase electoral de la segunda vuelta presidencial, al permitir determinar que los componentes de software utilizados durante la jornada correspondían efectivamente a las versiones previamente auditadas y autorizadas para su operación.

El procedimiento aplicado fue desarrollado de manera secuencial, orientado a establecer una línea base de confianza, verificar la correspondencia de los componentes desplegados en campo y validar la

permanencia de sus condiciones de integridad durante la operación electoral.

La primera fase correspondió al sellado de versiones y establecimiento de la línea base de referencia, ejecutada el 18 de junio de 2026. Durante esta actividad se participó en el procedimiento de registro y custodia del software destinado a operar durante la segunda vuelta presidencial, registrándose las versiones oficiales de los diferentes componentes, calculándose los valores criptográficos de referencia (hash) y documentándose los elementos de hardware asociados a la operación del sistema de escrutinios. Para los sistemas de Preconteo y Escrutinio se utilizaron registros SHA-256, mientras que para el Sistema de Consolidación y Divulgación se generaron registros SHA-512. Este proceso evidenció la concordancia de las versiones de software revisadas por la auditoría y las dispuestas para operación en la elección. El conjunto de estos elementos constituyó la línea base utilizada posteriormente por la auditoría para verificar la identidad de los componentes al inicio y final de la jornada electoral.

La segunda fase consistió en la verificación nacional de los equipos utilizados por las comisiones escrutadoras, ejecutada el 20 de junio de 2026. Como parte de este procedimiento se efectuaron validaciones presenciales en Antioquia, Atlántico, Bogotá D.C., Cundinamarca y Santander, mediante la ejecución de scripts automatizados orientados a extraer y contrastar los registros criptográficos de las versiones de software sobre los componentes instalados en campo. La revisión comprendió un total de 242 comisiones escrutadoras distribuidas en 102 comisiones de Medellín, 43 comisiones de Bogotá, 67 comisiones auxiliares de Barranquilla, 29 comisiones zonales de Bucaramanga y una comisión auxiliar en Cundinamarca.

Durante estas verificaciones se corroboró la correspondencia entre los equipos utilizados por las comisiones escrutadoras y los registros de hardware previamente inventariados durante el proceso de congelamiento de versiones. Esta actividad permitió fortalecer la trazabilidad entre los componentes de software auditados y la infraestructura física utilizada para su ejecución durante el proceso electoral.

La tercera fase se desarrolló el 21 de junio de 2026, durante la jornada electoral, en la que se realizó la verificación de las versiones de software sobre los sistemas puestos en producción. Para el Sistema de Preconteo se llevó a cabo en el Centro de Control Nacional, tomando un primer registro de huella criptográfica previo al inicio de la operación electoral y un segundo registro al cierre del proceso. De igual forma, para el Sistema de Consolidación y Divulgación se efectuaron verificaciones en el Centro de Gestión Nacional, con un primer registro de huellas criptográficas antes del inicio de la jornada y un segundo registro una vez finalizada la divulgación de resultados.

La aplicación de registros antes y después de la operación permitió verificar no solamente la identidad inicial de los componentes desplegados, sino también la permanencia de sus condiciones de integridad durante todo el ciclo operativo de la jornada electoral, incluyendo las fases de procesamiento y divulgación de resultados.

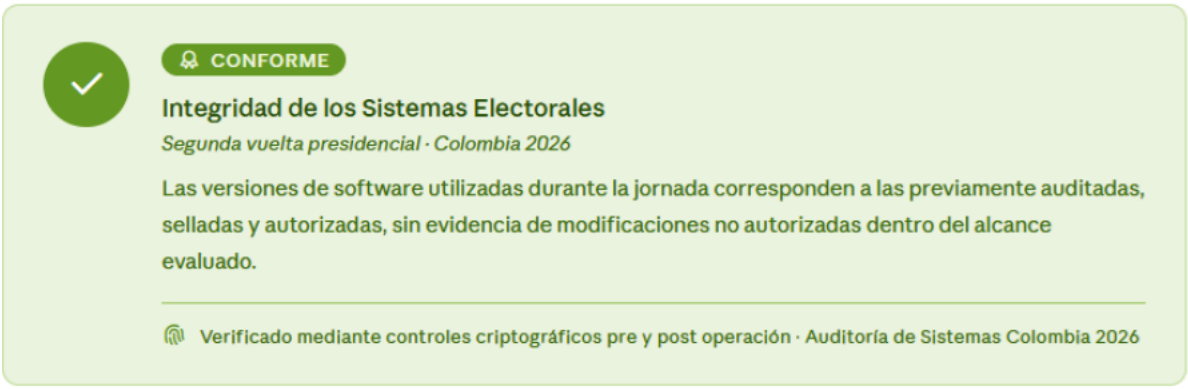
La fase final consistió en el contraste de los registros obtenidos durante las verificaciones de campo y durante la operación de los sistemas contra los valores de referencia generados durante el congelamiento de versiones. Para ello se revisaron componentes críticos asociados a los procesos de captura, interpretación, verificación, control operativo, escrutinio, monitoreo, generación de archivos y divulgación de resultados, así como los repositorios de fuentes y binarios correspondientes al Sistema de Consolidación y Divulgación.

Los resultados obtenidos evidenciaron una correspondencia plena entre los registros criptográficos de control y los registros generados durante las verificaciones efectuadas por la auditoría. Los once componentes contrastados presentaron coincidencia total con los valores de referencia establecidos en la línea base, incluyendo módulos utilizados para el procesamiento de información electoral, componentes de monitoreo operativo, herramientas de verificación, servicios de control y repositorios de software asociados a los sistemas evaluados.

No se identificaron diferencias que permitieran inferir alteraciones, sustituciones, inyecciones de código o modificaciones sobre los elementos evaluados. Asimismo, las verificaciones efectuadas antes, durante y después de la operación de los sistemas confirmaron la estabilidad de los componentes auditados durante todo el ciclo operativo de la jornada electoral.

La evidencia recopilada permite concluir que los componentes de software verificados durante la fase electoral mantuvieron sus condiciones de integridad y trazabilidad respecto de las versiones previamente auditadas, selladas y puestas en custodia. En consecuencia, las verificaciones efectuadas descartan, dentro del alcance evaluado, la existencia de modificaciones no autorizadas sobre los componentes analizados y aportan evidencia objetiva de que las versiones utilizadas durante la segunda vuelta presidencial corresponden a las mismas versiones previamente auditadas y autorizadas para su utilización durante el proceso electoral.

Resumen de resultados



7.2 Infraestructura Tecnológica y Disponibilidad Operativa

La infraestructura tecnológica desplegada para la segunda vuelta presidencial fue objeto de seguimiento y análisis con el fin de verificar las condiciones de disponibilidad, estabilidad operativa y continuidad de los servicios que soportaron los procesos de preconteo, escrutinio, consolidación y divulgación de resultados electorales.

La evaluación consideró el comportamiento de los canales nacionales de comunicación, las plataformas institucionales utilizadas durante la jornada, los servicios de procesamiento y publicación de información, así como las configuraciones críticas de infraestructura, bases de datos y componentes de conectividad asociados a la operación electoral. Asimismo, se revisaron registros operativos y evidencias generadas por las herramientas de monitoreo y administración de la infraestructura tecnológica.

El monitoreo efectuado sobre la red nacional de comunicaciones evidenció disponibilidad continua de los servicios durante toda la jornada electoral. Los 518 puntos supervisados mantuvieron condiciones normales de operación y permitieron la transmisión oportuna de la información requerida por los distintos componentes tecnológicos involucrados en el proceso electoral.

Los registros operativos evidencian la gestión de dos eventos asociados a servicios de telecomunicaciones durante la jornada electoral. Las acciones implementadas por los equipos responsables permitieron atender oportunamente las situaciones identificadas, preservando la continuidad de los servicios y manteniendo la disponibilidad de los componentes tecnológicos que soportaron el proceso electoral. No se registraron afectaciones sobre la operación de los sistemas evaluados ni interrupciones de los servicios críticos.

La observación de las plataformas institucionales permitió verificar el funcionamiento de 36 portales asociados al proceso electoral, incluyendo servicios de consulta ciudadana, preconteo, escrutinio, digitalización de formularios electorales, monitoreo operativo y divulgación de resultados. La evidencia revisada no mostró indisponibilidades ni degradaciones relevantes que comprometieran la prestación de dichos servicios durante el período evaluado.

Resultó relevante el comportamiento observado durante la franja comprendida entre las 16:00 y las 17:00 horas, período en el cual se concentraron las mayores exigencias operativas asociadas al cierre de mesas y a la divulgación de resultados preliminares. Durante este intervalo se registraron volúmenes de tráfico cercanos a los 756 millones de solicitudes y tasas de procesamiento aproximadas de 262 millones de solicitudes por minuto, manteniéndose la estabilidad de los servicios y la capacidad de respuesta de la infraestructura tecnológica.

Las revisiones efectuadas sobre componentes de infraestructura incluyeron la validación de configuraciones de dispositivos de seguridad, bases de datos, servicios de distribución de contenido y plataformas desplegadas en las diferentes regiones operativas. De igual forma, se analizaron registros de auditoría provenientes de AWS CloudTrail, evidenciándose 8.428 eventos de gestión asociados principalmente a procesos de autenticación, administración de instancias y generación de registros operativos, sin identificarse actividades incompatibles con la operación normal de la plataforma.

La evidencia obtenida a partir de los registros de auditoría (AWS CloudTrail), los servicios de distribución de contenido (CloudFront), los mecanismos de protección perimetral (Nexus Guard) y las plataformas de soporte a la operación permitió corroborar que el entorno tecnológico utilizado durante la jornada electoral conservó las condiciones técnicas previamente evaluadas por la auditoría. Los análisis efectuados no evidenciaron modificaciones no autorizadas o alteraciones sobre la infraestructura tecnológica que soportó la operación electoral, ni desviaciones respecto de la arquitectura, configuraciones y procedimientos de administración establecidos para los componentes evaluados. Estos resultados proporcionan evidencia objetiva de que la plataforma tecnológica operó bajo condiciones de control, trazabilidad y gobernabilidad técnica durante todo el período evaluado.

La infraestructura tecnológica mantuvo condiciones adecuadas de disponibilidad, estabilidad y capacidad operativa durante toda la jornada electoral, incluyendo los períodos de mayor demanda observados. Los mecanismos de monitoreo, redundancia y administración implementados permitieron sostener la continuidad de los servicios críticos sin afectaciones para la operación electoral.

Con fundamento en las verificaciones efectuadas, se concluye que la infraestructura tecnológica presentó un comportamiento estable y consistente con los requerimientos operativos de la segunda vuelta presidencial, manteniendo la disponibilidad de los servicios críticos y la continuidad de las operaciones durante todo el período evaluado.

Resumen de resultados

CONFORME

Infraestructura Tecnológica y Disponibilidad Operativa

Segunda vuelta presidencial · Colombia 2026

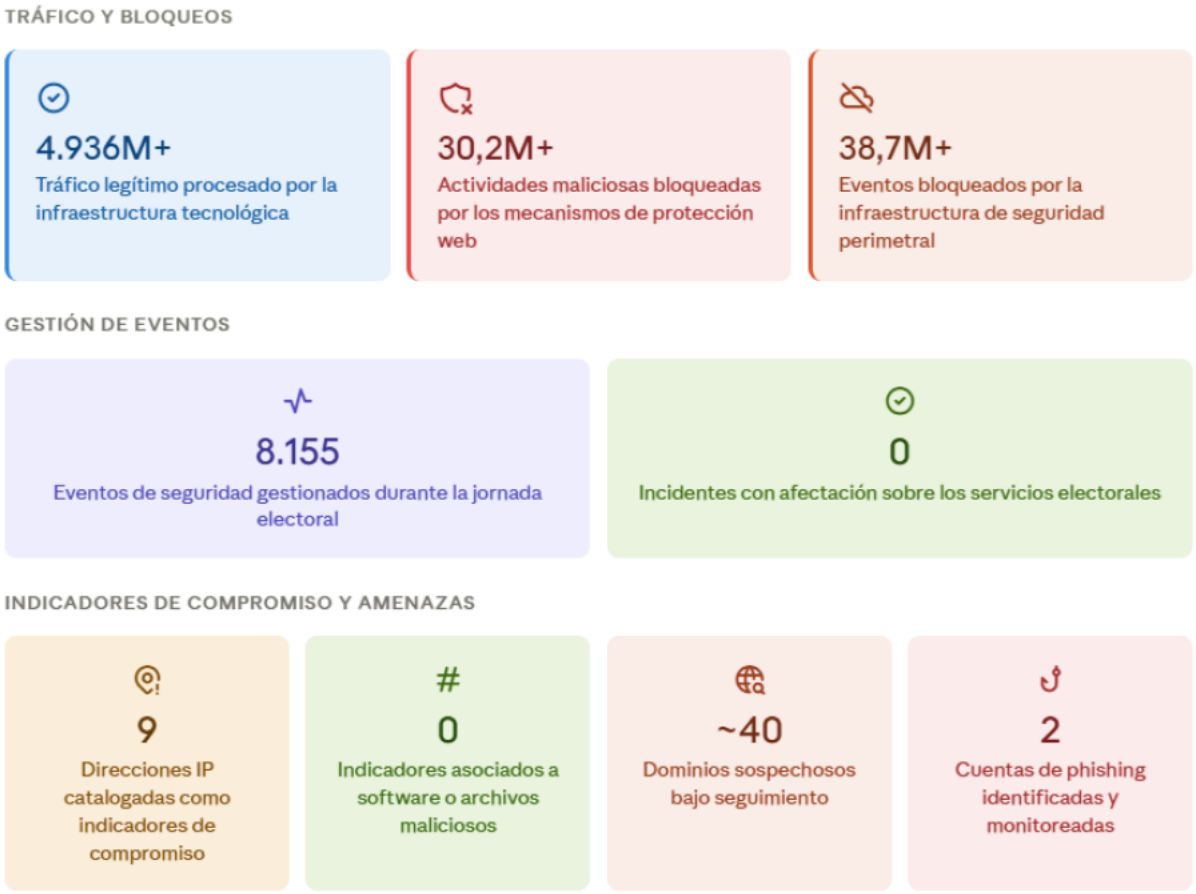
La infraestructura tecnológica presentó un comportamiento estable y consistente con los requerimientos operativos, manteniendo la disponibilidad de los servicios críticos y la continuidad de las operaciones durante todo el período evaluado.

Verificado mediante monitoreo continuo · Auditoría de Sistemas Colombia 2026

7.3 Monitoreo de Seguridad y Protección de Servicios

La protección de los servicios electorales se sustentó en un esquema de seguridad multinivel conformado por mecanismos de protección perimetral, monitoreo continuo, inteligencia de amenazas y gestión de eventos de seguridad, operados de manera coordinada por los diferentes centros de monitoreo y respuesta involucrados en la operación electoral.

La evaluación realizada consideró la información generada por los mecanismos de protección implementados sobre la infraestructura tecnológica, los servicios expuestos a Internet y los componentes críticos del proceso electoral, incluyendo plataformas de preconteo, escrutinio, consolidación, divulgación de resultados y servicios institucionales asociados.



Los registros analizados evidencian una actividad significativa sobre los mecanismos de protección desplegados durante la jornada electoral. Los servicios tecnológicos procesaron más de 4.936 millones de solicitudes legítimas, manteniendo una tasa de éxito cercana al 98,9%, mientras que los controles de seguridad bloquearon más de 30,2 millones de solicitudes maliciosas dirigidas a los portales y servicios expuestos a Internet.

Los mecanismos de protección implementados sobre componentes de infraestructura y servicios on-premise bloquearon aproximadamente 38,7 millones de eventos adicionales asociados a actividades potencialmente maliciosas, evidenciando una actividad constante de filtrado y contención durante todo el período evaluado.

El análisis de los eventos gestionados muestra que las principales actividades detectadas correspondieron a intentos de denegación de servicio, tráfico automatizado mediante bots y conexiones originadas desde direcciones IP incluidas en fuentes de inteligencia de amenazas. Los registros revisados indican que estos eventos fueron identificados, clasificados y tratados por los mecanismos de protección implementados, sin generar afectaciones sobre la disponibilidad o funcionamiento de los servicios electorales.

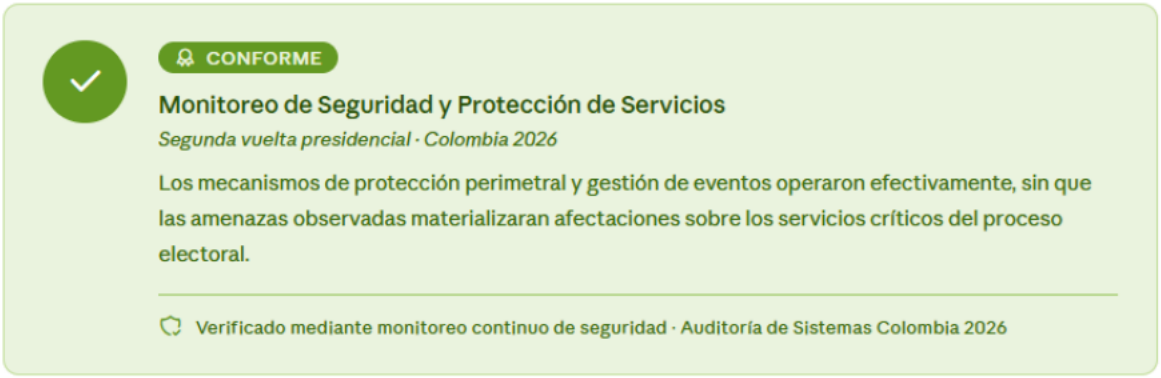
Durante la jornada se gestionaron 8.155 eventos notables de seguridad sin impacto operativo. Asimismo, el seguimiento efectuado sobre indicadores de compromiso permitió identificar nueve direcciones IP de interés para el análisis de amenazas, aproximadamente cuarenta dominios sospechosos y dos cuentas asociadas a actividades de phishing, elementos que fueron incorporados a los procesos de vigilancia y seguimiento desarrollados por los equipos responsables de la seguridad tecnológica.

No se evidenciaron incidentes críticos de ciberseguridad, compromisos de integridad sobre los sistemas evaluados, afectaciones a la disponibilidad de los servicios electorales ni eventos de exfiltración de información asociados a la segunda vuelta presidencial. De igual forma, no se identificó

materialización de los ataques anunciados por actores observados durante las actividades de vigilancia digital.

Los resultados obtenidos permiten concluir que los mecanismos de monitoreo, protección perimetral y gestión de eventos operaron de manera efectiva durante la jornada electoral, proporcionando capacidades adecuadas de detección, prevención y respuesta frente a las amenazas observadas, sin que se materializaran afectaciones sobre los servicios críticos que soportaron el proceso electoral.

Resumen de resultados

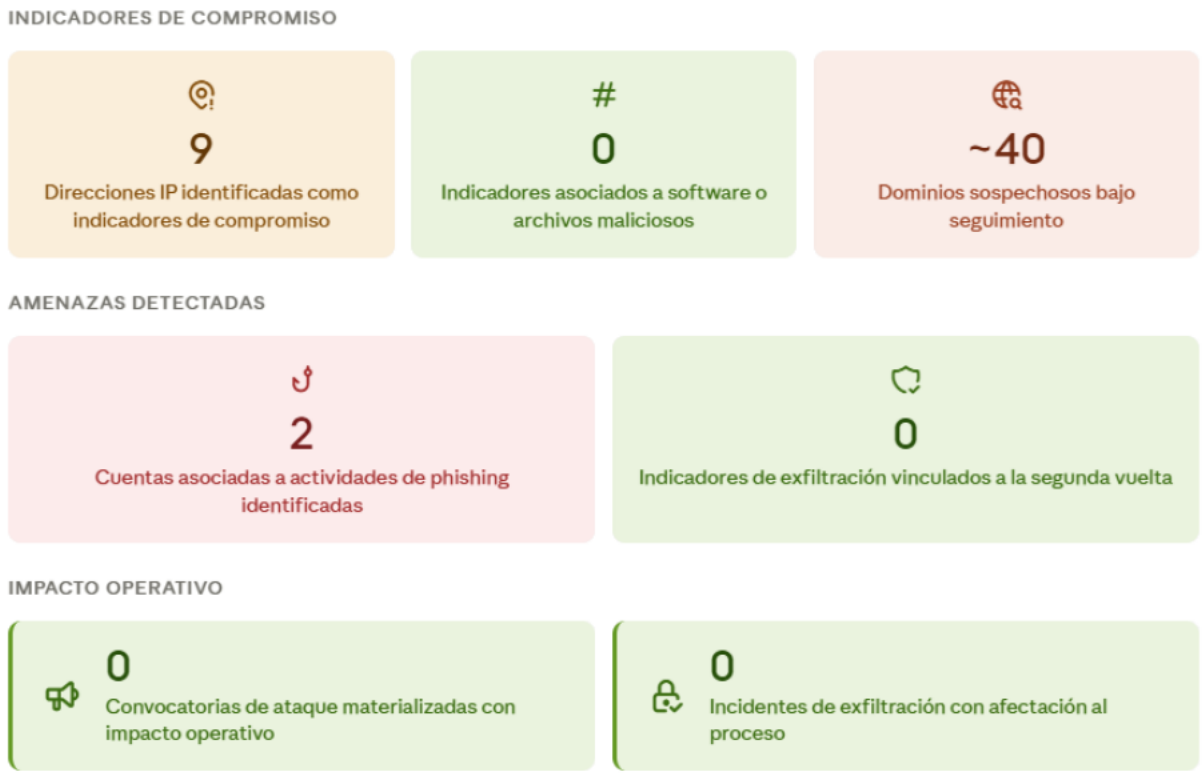


7.4 Gestión de Amenazas e Inteligencia de Seguridad

La protección del proceso electoral no se limitó a la detección y bloqueo de actividades maliciosas sobre la infraestructura tecnológica, sino que incorporó actividades permanentes de vigilancia, análisis e inteligencia orientadas a identificar amenazas emergentes que pudieran afectar la disponibilidad de los servicios, la integridad de la información electoral o la confianza pública en los resultados del proceso.

Las actividades desarrolladas contemplaron el seguimiento de indicadores de compromiso, el monitoreo de fuentes abiertas, redes sociales, espacios de intercambio en internet y otras fuentes de inteligencia utilizadas para

identificar posibles campañas de ataque, actividades de hacktivismo, intentos de phishing, procesos de desinformación y otros eventos potencialmente relevantes para la seguridad del proceso electoral.



Se evidenció que las actividades de vigilancia permitieron identificar un conjunto limitado de indicadores de compromiso asociados principalmente a direcciones IP y dominios potencialmente relacionados con actividades de reconocimiento, monitoreo o generación de tráfico malicioso. No obstante, los análisis efectuados no identificaron evidencias de compromiso efectivo sobre los sistemas electorales ni actividades que afectaran la operación de los servicios observados.

Los registros analizados tampoco evidenciaron procesos de exfiltración de información asociados a la segunda vuelta presidencial. De acuerdo con la información suministrada por los diferentes equipos de monitoreo, los eventos observados correspondieron principalmente a reutilización o redistribución de información previamente conocida, sin identificarse

filtraciones nuevas relacionadas con los sistemas o componentes evaluados durante esta etapa.

De igual forma, las actividades de vigilancia permitieron identificar manifestaciones públicas y anuncios relacionados con posibles acciones de hacktivismo dirigidas contra la infraestructura electoral. Sin embargo, la evidencia recopilada no mostró la materialización de dichos anuncios ni la ejecución de acciones que generaran afectaciones sobre los servicios tecnológicos que soportaron el proceso electoral.

Un aspecto relevante observado durante esta jornada corresponde al desplazamiento del riesgo desde escenarios predominantemente tecnológicos hacia escenarios asociados a la desinformación. Los principales eventos observados estuvieron relacionados con la difusión de narrativas sobre presunto fraude electoral a través de redes sociales y otros medios digitales. Frente a este escenario, los mecanismos de trazabilidad, verificación de integridad e inmutabilidad de software e infraestructura constituyeron elementos objetivos para sustentar técnicamente la confiabilidad de los sistemas utilizados durante la jornada.

La información obtenida a partir de las diferentes fuentes de monitoreo muestra una elevada consistencia entre los análisis efectuados por los SOC. Los reportes generados por estas instancias coinciden en la ausencia de incidentes críticos, la disponibilidad continua de los servicios tecnológicos y la efectividad de los mecanismos de protección implementados para la gestión de las amenazas observadas durante la jornada electoral.

Esta convergencia de resultados fortalece el nivel de confianza sobre las conclusiones obtenidas, al provenir de fuentes independientes que realizaron actividades complementarias de monitoreo, vigilancia, correlación de eventos e inteligencia de amenazas sobre diferentes componentes de la infraestructura tecnológica electoral.

Con fundamento en la evidencia analizada, se concluye que las actividades de vigilancia, inteligencia y gestión de amenazas permitieron identificar

oportunamente los riesgos relevantes para la jornada electoral y mantener una adecuada capacidad de detección y seguimiento sobre los eventos observados, sin evidenciarse amenazas materializadas que comprometieran la operación tecnológica o la integridad de los sistemas electorales evaluados.

Resumen de resultados

CONFORME

Gestión de Amenazas e Inteligencia de Seguridad

Segunda vuelta presidencial · Colombia 2026

Las actividades de vigilancia e inteligencia permitieron identificar oportunamente los riesgos relevantes, sin que se materializaran amenazas que comprometieran la operación tecnológica o la integridad de los sistemas evaluados.

Verificado mediante análisis de inteligencia y vigilancia continua · Auditoría de Sistemas Colombia 2026

VIII. CONCLUSIONES

La evidencia obtenida durante el día de las elecciones de la segunda vuelta presidencial permitió verificar, desde diferentes perspectivas técnicas y operativas, las condiciones bajo las cuales fueron utilizados los sistemas de información y la infraestructura tecnológica que soportaron el proceso electoral.

Las verificaciones realizadas proporcionaron evidencia consistente y suficiente para sustentar las valoraciones efectuadas durante la auditoría, asimismo, los resultados observados mantuvieron coherencia entre las distintas fuentes de información analizadas.

De manera particular, la aplicación de procedimientos de verificación sobre software, infraestructura tecnológica, mecanismos de protección y fuentes de monitoreo permitió disponer de elementos objetivos para valorar el comportamiento de los sistemas durante la jornada electoral y reducir la incertidumbre asociada a los riesgos tecnológicos inherentes a este tipo de procesos.

La evidencia recopilada durante la auditoría no mostró situaciones que comprometieran el adecuado funcionamiento de los servicios tecnológicos utilizados para soportar el procesamiento, escrutinio, consolidación y divulgación de resultados electorales. Asimismo, los controles observados durante la evaluación evidenciaron niveles adecuados de capacidad operativa, protección y respuesta frente a los eventos registrados durante el período analizado.

Con fundamento en la totalidad de la evidencia examinada, la auditoría concluye que los componentes tecnológicos incluidos dentro del alcance de evaluación operaron durante la segunda vuelta presidencial bajo condiciones compatibles con los requerimientos funcionales, operativos y de seguridad establecidos para el proceso electoral, sin identificarse situaciones que comprometieran de manera significativa la integridad, disponibilidad o continuidad de los servicios tecnológicos evaluados.

IIDH / CAPEL