BOLETÍN PMU CENTRAL — Nro. [002] – [16:00]

31 de mayo de 2026

SECCIÓN I — ESTADO GENERAL DE LA JORNADA

Indicador	**ESTABLE**
Entidad Reportante	PMU Ciber Electoral 2026 – Elecciones Presidenciales
Hora del corte	**16:00 p.m.**

SECCIÓN II — RESUMEN EJECUTIVO

Al cierre de la *jornada electoral presidencial del 31 de mayo de 2026*, el componente digital del proceso concluye estable y sin afectaciones que hayan comprometido la continuidad de los comicios ni la integridad del proceso. A lo largo de todos los cortes —desde la apertura en la madrugada hasta el cierre de las urnas— el estado se mantuvo de forma consistente, y la fase de preconteo se desarrolla con normalidad.

La infraestructura electoral conservó alta resiliencia operativa de principio a fin. El tráfico ciudadano alcanzó su pico en la mañana, en las horas de mayor consulta, y descendió de forma progresiva durante la tarde dentro de los niveles esperados, manteniendo en todo momento disponibilidad y navegación fluida. El monitoreo confirmó comportamiento normal en los 28 centros de procesamiento de datos, las 32 salas de prensa y las plataformas de preconteo y E-14. No se registraron incidentes cibernéticos que afectaran los sistemas electorales, y la Fiscalía General de la Nación reportó que no se presentaron denuncias por delitos informáticos a nivel nacional.

Las amenazas detectadas durante la jornada fueron identificadas, contenidas y gestionadas oportunamente mediante la articulación interinstitucional, sin que ninguna comprometiera la operación electoral. Entre ellas se atendieron dominios que suplantaban a la Registraduría, direcciones de internet maliciosas reportadas por la Registraduría y la Procuraduría —validadas y bloqueadas de forma preventiva—, la validación conjunta con la Rama Judicial y la Fiscalía sobre información presuntamente expuesta, y la publicación involuntaria de un informe reservado por parte del Ministerio de Justicia. En materia de desinformación, se mantuvo el monitoreo permanente de las narrativas circulantes, sin que se configuraran campañas con impacto determinante sobre el desarrollo del proceso.

El PMU Ciber Electoral cumplió su rol de monitoreo, anticipación y respuesta coordinada entre entidades durante toda la jornada, garantizando la protección del componente

digital de los comicios. La instancia mantendrá el seguimiento durante el preconteo y el escrutinio para asegurar una respuesta oportuna

ante cualquier eventualidad posterior al cierre.

SECCIÓN III — SITUACIÓN POR DOMINIO.

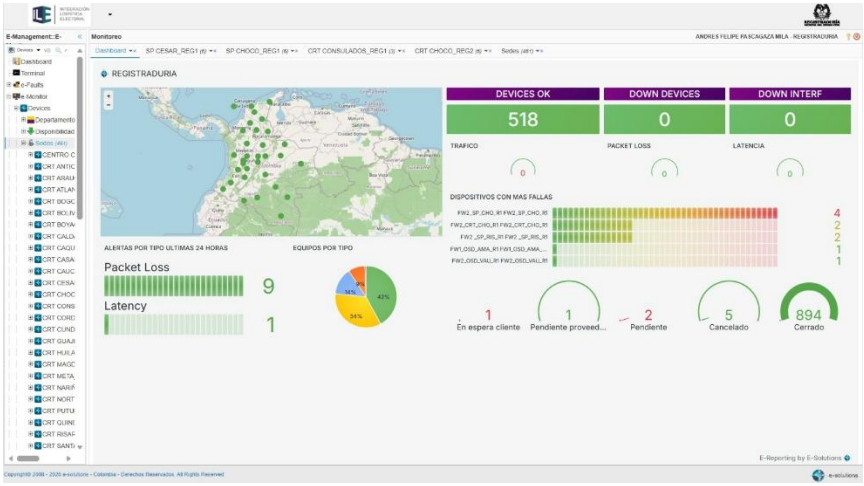
1. **D1 — Disponibilidad de sistemas electorales – (**Fuente RNEC**):**

La infraestructura tecnológica del componente electoral presenta una alta resiliencia operativa. Los niveles de tráfico se mantienen dentro de los umbrales de seguridad, permitiendo una navegación fluida para la ciudadanía.

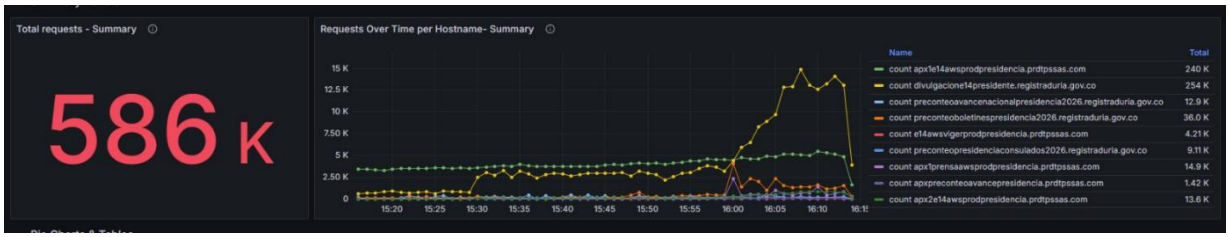
Consolidado de peticiones — Registraduría (31 de mayo de 2026)

Hora	Elecciones Colombia	Areportar	Areportar App
10:37	57.8 millones	19 mil	22.6 mil
11:28	20.5 millones	5.40 mil	3.93 mil
13:20	15.4 millones	2.87 mil	2.22 mil
14:20	12.9 millones	8.25 mil	7.19 mil
15:20	8.34 millones	5.02 mil	4.03 mil

El comportamiento del tráfico refleja un pico en horas de la mañana —cuando se concentró la mayor consulta ciudadana— y un descenso progresivo durante la tarde, dentro de los niveles esperados. Las plataformas mantuvieron disponibilidad y navegación fluida en todo momento, sin afectaciones.



Revisado el portal de monitoreo de la Registraduría de los 28 centros de procesamiento de datos CRT, y de las 32 sala de prensa se observa un comportamiento normal en la infraestructura tecnológica en cada uno de los puntos.



Se observa un comportamiento normal en la plataforma preconteo y E14.

2. **D2 — Incidentes gestionados:** Sin novedad.

3. **D3 — Denuncias y evidencia digital – (**Fuente DIJIN /Fiscalía**):**

   La Fiscalía General de la Nación informa que no se presentó denuncias relacionadas con delitos informático a nivel nacional

4. **D4 — Amenazas identificadas - (**Fuente ColCERT, CCOCI, CECIP, PONAL**):**

- La Registraduría reportó seis direcciones de internet identificadas como peligrosas, asociadas a programas maliciosos diseñados para tomar control remoto de equipos (tipo RAT). Estas direcciones fueron analizadas y confirmadas como maliciosas por inteligencia de amenazas, y ya se incorporaron a los mecanismos de bloqueo preventivo para impedir cualquier intento de afectación a los sistemas electorales durante la jornada.

- La Procuraduría reportó una dirección de internet peligrosa, vinculada a intentos de acceso no autorizado mediante prueba masiva de contraseñas y rastreo de servicios de conexión remota. Tras su validación como maliciosa, la dirección fue incorporada igualmente a las medidas de bloqueo preventivo. Estas acciones refuerzan la protección de la infraestructura digital y evidencian la articulación oportuna entre las entidades y el PMU Ciber Electoral.

- La Rama Judicial sigue evaluando de manera conjunta con la Fiscalía General de la Nación, la información reportada como expuesta para identificación del repositorio.

5. **D5 — Protección de sistemas:** Sin novedad

6. **D6 — Desinformación - (**Fuente ColCERT, CCOCI, CECIP, DNI**):**

- Las cadenas de desinformación son una constante en las jornadas electorales. Desplegadas estratégicamente a favor y en contra de todos los candidatos, su objetivo es claro: saturar el debate público, contaminar el entorno mediático y manipular la decisión del elector. Sin embargo, más que un patrón masivo y centralizado, estas campañas operan como tácticas fragmentadas de soft power, diseñadas para moldear percepciones de forma sutil pero persistente.

SECCIÓN IV — MEDIDAS DE PROTECCIÓN ADOPTADAS
Las medidas de protección vigentes se mantienen sin cambios.

SECCIÓN V — CONCLUSIÓN ESTRATÉGICA: Sin novedad

SECCIÓN VI — SEGUIMIENTO A CORTES ANTERIORES

Situación	Acción	Estado actual
Actividad maliciosa confirmada, atribuida a un actor de perfil hacktivista, con evidencia de recopilación y posible exposición de información de entidades gubernamentales. Validado mediante OSINT y correlación de fuentes.	☑ Notificación a RNEC ☑ Otra: validación técnica interna de la supuesta exposición de bases de datos y verificación de integridad de la información institucional.	En Proceso
Identificación de cuatro dominios externos que suplantan o imitan a la Registraduría Nacional del Estado Civil: (registraduria-col-org[.]com, registradurianacional[.]com,juradoregnacional[.]com y registraduriagov[.]ph), con infraestructura preparada para activación o uso fraudulento. Los sistemas de la entidad no presentan compromiso confirmado.	☑ Notificación a la RNEC mediante informe técnico. ☑ Recomendación de reporte a proveedores y bloqueo preventivo en plataformas de seguridad. ☑ Vigilancia de activación durante la jornada.	En gestión de bloqueo / validación con la entidad.

Posible exfiltración de información del 30 de mayo de 2026, que involucraría datos asociados a la Rama Judicial.	☑ Mesa técnica con la Rama Judicial para validar la información expuesta. ☑ Verificación interna en cada entidad para confirmar si los datos corresponden a sus sistemas.	En Proceso
Se evidenció la publicación de un informe de gestión de vulnerabilidades remitido por el ColCERT en un portal institucional de acceso público —en la sección de resoluciones—. El documento contiene información sensible y de acceso restringido relacionada con vulnerabilidades identificadas en infraestructura tecnológica. La divulgación involuntaria de esta información podría incrementar la exposición al riesgo, al facilitar que terceros identifiquen y aprovechen posibles debilidades de seguridad asociadas a los sistemas referenciados en el informe.	☑ Notificación a la entidad para el retiro inmediato del documento. ☑ Verificación de su posible difusión y alcance.	En proceso de notificación, retiro y contención.