BOLETÍN PMU CENTRAL — Nro. [08] Segunda vuelta

## Resumen ejecutivo

21 de junio de 2026

**SECCIÓN I — ESTADO GENERAL DE LA JORNADA**

| | |
|---|---|
| **Indicador** | **ESTABLE EN OBSERVACION** |
| **Entidad Reportante** | PMU Ciber Electoral 2026 – Elecciones Presidenciales – Segunda Vuelta |
| **Hora del corte** | **04:00 p.m** |

**CONTEXTO:**

El PMU Ciber Electoral se consolida como el eje estratégico fundamental para blindar la infraestructura crítica del Estado durante los comicios, sustentando su actuación en el Artículo 2.2.21.1.3.9 del Título Primero del Decreto 1078 de 2015 que adiciona el Decreto 338 de 2022. Esta base legal lo define como la instancia legítima de colaboración y coordinación interinstitucional para articular y facilitar la toma de decisiones estratégicas y operacionales ante incidentes cibernéticos.

Gracias a este respaldo normativo, la articulación de las instancias ciber del Estado se ejecuta bajo un estricto cumplimiento constitucional y legal, promoviendo el respeto y protección de los derechos humanos y la garantía de los derechos ciudadanos en el ciberespacio. Al centralizar el reporte y flujo de información a través de canales oficiales y estructurados, el PMU Ciber Electoral optimiza la capacidad de respuesta oportuna mediante datos accionables, mitigando riesgos en tiempo real y neutralizando vectores de amenaza que pretendan desestabilizar la jornada en las regiones.

En última instancia, esta sinergia institucional y su riguroso marco jurídico son los pilares que salvaguardan la transparencia de las actividades, que apoyan la validación de la normalidad de los sistemas de votación y escrutinio para proyectar una sólida confianza en la seguridad digital a nivel nacional y territorial.

**SECCIÓN II — RESUMEN EJECUTIVO**

Al corte de las 16:00, la jornada se mantiene tecnológicamente estable y sin incidentes cibernéticos sobre la infraestructura electoral; los portales de la RNEC conservan su disponibilidad y el CNE opera con normalidad.

El hallazgo principal del corte es un intento de automatización y recolección de información. El CCOCI advierte sobre el desarrollo de herramientas orientadas a la extracción masiva, en búsqueda de posibles debilidades en los controles de límite de peticiones. De forma concordante, la Policía Nacional identificó en fuentes abiertas un repositorio público que aloja una herramienta para descarga masiva.

Ambos hallazgos, no constituyen evidencia de compromiso de los sistemas internos de la RNEC, dado que operan sobre información ya publicada. La desinformación se mantiene como riesgo de fondo, con narrativas de presunto fraude en puestos de votación y de presunto constreñimiento electoral y presión territorial, todas en monitoreo preventivo y pendientes de verificación oficial.

**SECCIÓN III — SITUACIÓN POR DOMINIO**.

1. **D1 — Disponibilidad de sistemas electorales – (**Fuente RNEC- CNE**):** Sin novedad.

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

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

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

El CCOCI advierte sobre el desarrollo de herramientas orientadas a la extracción masiva en búsqueda de posibles debilidades en los controles de límite de peticiones en portales el sector electoral. De forma concordante, la Policía Nacional identificó en fuentes abiertas un repositorio público que aloja una herramienta para descarga masiva. No se identifican, de forma concluyente, indicios de una brecha directa ni compromiso de las bases de datos internas. Estado: en análisis preventivo; se solicita a la RNEC notificación y validación técnica interna. **Fuente: CCOCI.**

La Policía Nacional reportó, mediante monitoreo de fuentes abiertas, la identificación de un repositorio público que aloja una herramienta automatizada para la descarga masiva en un municipio directamente desde el Visor Ciudadano de la Registraduría, el repositorio es de creación reciente y de baja difusión al corte. No constituye, por sí mismo, evidencia de compromiso de los sistemas internos de la RNEC, dado que opera sobre información publicada. Acciones: Notificación a la RNEC para validación y endurecimiento de controles Estado: en gestión solicitada. **Fuente: PONAL — OSINT / ColCERT.**

5. **D5 — Protección de sistemas: (Fuente CCOCI)**

Derivado del hallazgo anterior, el CCOCI recomienda robustecer la postura perimetral y los controles de los portales de consulta pública, formularios de validación de identidad y repositorios de E-14) Estado: acciones correctivas recomendadas / en validación. **Fuente: CCOCI.**

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

El CCOCI mantiene en monitoreo dos narrativas. La primera, sobre presunto fraude en puestos de votación (tarjetones presuntamente marcados, material proselitista en mesas, supuestas maletas con votos,difundida en X con fotografías y videos sin contexto completo que requieren verificación oficial. La segunda, sobre presunto constreñimiento electoral y

presión territorial. Ambas pueden incrementar la desconfianza institucional si se amplifican sin validación. Estado: en observación / monitoreo preventivo; se recomienda contrastar con RNEC, CNE, Procuraduría, Fiscalía, Defensoría y MOE. **Fuente: CCOCI.**

**SECCIÓN IV — MEDIDAS DE PROTECCIÓN ADOPTADAS**

Durante el corte, las instancias del PMU Ciber Electoral sostuvieron un esquema articulado de monitoreo y respuesta. Se destacan:

- Recomendaciones de endurecimiento de la postura perimetral, control estricto y monitoreo.
- Monitoreo preventivo del ecosistema de desinformación, con contraste interinstitucional (RNEC, CNE, Procuraduría, Fiscalía, Defensoría y MOE) sobre las narrativas de fraude y constreñimiento.
- Continuidad del monitoreo de disponibilidad de los portales electorales (SOC RNEC) y de la postura general de seguridad.

**SECCIÓN V — CONCLUSIÓN ESTRATÉGICA:**

La jornada se mantiene sólida en lo técnico, sin incidentes ni afectaciones de disponibilidad. El foco de este corte se desplaza hacia la protección de los datos electorales.

La prioridad estratégica es doble: de un lado, la validación técnica y el endurecimiento por parte de RNEC, del repositorio, antes de que la herramienta se difunda o se replique; del otro, la protección de la disponibilidad del portal, dado que una extracción masiva podría degradar el servicio y dar falsa veracidad a la narrativa del "cambiazo". En paralelo, se mantiene el monitoreo preventivo de las narrativas de presunto fraude y constreñimiento, con verificación interinstitucional antes de cualquier tratamiento como hecho confirmado.