BOLETÍN PMU CENTRAL — Nro. [09] 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	**06:00 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 cierre, la jornada electoral de la Segunda Vuelta Presidencial concluye sin novedades en ninguno de los dominios monitoreados. La infraestructura electoral se mantuvo estable y disponible durante toda la jornada, sin incidentes cibernéticos que comprometieran los activos del certamen.

En el balance de la operación, la RNEC sostuvo el 100% de disponibilidad en sus portales y los mecanismos de protección mitigaron de forma automatizada los ataques perimetrales, sin afectación del servicio; el CNE operó con normalidad durante todo el día. El principal vector de riesgo fue la desinformación —narrativas de presunto fraude, dominios de suplantación, cuentas de phishing y herramientas de extracción masiva de

información electoral—, atendido con monitoreo preventivo y articulación interinstitucional, sin que se confirmara compromiso de los sistemas internos de la RNEC.

El PMU Ciber Electoral mantiene la postura preventiva durante la fase de escrutinio y la consolidación oficial de resultados por parte de la autoridad electoral.

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): Sin novedad.**

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

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

SECCIÓN IV — MEDIDAS DE PROTECCIÓN ADOPTADAS

A lo largo de la jornada, las instancias del PMU Ciber Electoral sostuvieron un esquema articulado de monitoreo y respuesta. En el balance de la operación se destacan:

- Monitoreo permanente de la disponibilidad de los portales electorales (SOC RNEC), sin afectación del servicio.
- Gestión de dominios de suplantación, IP maliciosas y cuentas de phishing.
- Monitoreo preventivo del ecosistema de desinformación, con remisión de contenidos para verificación y articulación con RNEC, CNE, Procuraduría, Fiscalía, Defensoría y MOE.
- Notificación a la RNEC y recomendaciones de endurecimiento. Sostenimiento del esquema de coordinación interinstitucional del PMU y de los canales oficiales de reporte hasta el cierre de la jornada.

SECCIÓN V — CONCLUSIÓN ESTRATÉGICA:

La jornada electoral concluye con un balance positivo en materia de ciberseguridad: la infraestructura del proceso se comportó sólida y resiliente, sin incidentes ni afectaciones de disponibilidad, y con los vectores de ataque perimetral neutralizados de forma automatizada. Esto confirma la efectividad de la articulación interinstitucional y de los controles preventivos desplegados.

Se recomienda a las instancias ciber, continuar con el monitoreo frente a posibles amenazas a entidades gubernamentales.