BOLETÍN PMU CENTRAL — Nro. [07] 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	**02:00 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

El balance del corte refleja una jornada tecnológicamente estable y sin incidentes cibernéticos sobre la infraestructura electoral. La RNEC mantiene el 100% de disponibilidad en sus 36 portales, con más de 54 millones de solicitudes procesadas en el último corte (97,2% de éxito) y más de 777 mil eventos bloqueados preventivamente; a lo largo de la jornada se neutralizaron de forma automatizada los intentos de denegación de servicio (DoS) sin afectación del servicio. El CNE opera con normalidad.

La vigilancia se concentra en la periferia y el factor humano: se mantienen en seguimiento un nuevo dominio de suplantación de la Registraduría —detectado por ColCERT, ya inactivo y con bloqueo preventivo solicitado—, un conjunto de dominios fraudulentos,

direcciones IP maliciosas y cuentas de phishing, todo bajo monitoreo y sin compromiso confirmado.

El principal riesgo de la jornada - *la desinformación*. Se observa alta circulación de narrativas de presunto fraude contra la Registraduría, entre las que destaca una de mayor consistencia sobre un presunto "cambiazo" de resultados que se activaría ante una eventual caída o lentitud del portal. El PMU Ciber Electoral mantiene el monitoreo preventivo y recomienda blindar comunicacionalmente la disponibilidad del sistema de resultados.

SECCIÓN III — SITUACIÓN POR DOMINIO.

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

En el último corte (ventana 11:30–13:30, Informe N°14) se procesaron aproximadamente 54,6 millones de solicitudes, con una tasa de éxito cercana al 97,2%. El portal registraduria.gov.co registró 50,2 millones de solicitudes con 744 mil eventos bloqueados a nivel de firewall de red, sin eventos ni ataques de tipo DoS o WAF; resultados, 4,3 millones de solicitudes y 28,6 mil bloqueados; descargas, 50,9 mil y 4,2 mil bloqueados; SAC, 1,9 mil y 27 bloqueados. En conjunto, los mecanismos de protección bloquearon más de 777 mil solicitudes, sin afectar la continuidad ni el desempeño de los servicios.

De forma acumulada en la jornada (ventana 00:00–11:30, Informe Consolidado N°2), el portal liviano había procesado más de 111,4 millones de solicitudes permitidas (WAF bloqueó 2.327.478 maliciosas) y, en el aplicativo aVotar, la nube segura bloqueó 12.551.853 eventos —incluidos 4.626.260 de tipo DoS— sin afectación del servicio. Estado: **ESTABLE / sin novedad**. **Fuente: RNEC (SOC).**

El CNE reporta operación normal de sus servicios tecnológicos, con 100% de disponibilidad (*uptime*) y picos de tráfico de 168 Mbps al corte de las 13:00. **Fuente: CNE.**

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

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

El CECIP – Centro Cibernético Policial, en el marco del Plan Democracia, reporta actividad de ciberpatrullaje con 05 alertas remitidas, 16 contenidos preventivos y 04 preservaciones de publicaciones, sin incidentes cibernéticos sobre los activos del certamen electoral. Adicionalmente, se dio trámite ante los entes judiciales para la verificación de publicaciones en X que difundían presunto material visual de un grupo de WhatsApp. **Fuente: CECIP – PONAL.**

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

Durante la jornada, el ColCERT detectó un nuevo dominio de suplantación de la Registraduría. Al momento de la validación pasiva, el dominio no presenta historial de certificados, escaneos ni snapshots, consistente con un endpoint efímero creado y

eliminado. Se solicitó a la RNEC comunicación oficial de desmentido, bloqueo preventivo Estado: en monitoreo / bloqueo preventivo solicitado. **Fuente: ColCERT.**

El SOC de la RNEC reporta, a partir de inteligencia de amenazas la detección de direcciones IP clasificadas como maliciosas/IoC con tráfico sospechoso hacia plataformas del proceso, sin compromiso confirmado. Mantiene en seguimiento cuentas de phishing que suplantan a jurados Estado: en monitoreo / seguimiento. **Fuente: RNEC (SOC).**

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

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

El CECIP – Centro Cibernético Policial reporta, en su corte de las 12:00, monitoreo activo del ecosistema de desinformación: 16 contenidos preventivos publicados y un alcance potencial superior a 100 millones de interacciones en redes sociales, con alta actividad de tendencias asociadas a ambas campañas en X. Se identificó la difusión en YouTube de un video con el testimonio anónimo de una persona que se presenta como presunta funcionaria de la Registraduría Nacional, exponiendo presuntas irregularidades del proceso de segunda vuelta; la alerta fue remitida al ColCERT para su evaluación. El caso se mantiene en monitoreo y verificación. **Fuente: CECIP – PONAL.**

El servicio de Vigilancia Digital de la RNEC califica el riesgo como **BAJO**, con alta concentración de publicaciones que cuestionan la transparencia de la Registraduría y promueven narrativas de presunto fraude (reedición de "muertos que votan" y "software electoral"). Destaca una narrativa de mayor consistencia sobre un presunto **"cambiazo" de la base de datos de resultados** que se ejecutaría aprovechando una eventual caída o lentitud del portal; por su diseño, una indisponibilidad temporal por alta demanda podría usarse para dar falsa veracidad a la teoría, por lo que se recomienda comunicación preventiva. Se observan además señalamientos sobre presuntas irregularidades en puestos, compra de votos, doble voto, presiones a jurados y mensajes falsos que desincentivan el voto en segunda vuelta. Los 36 portales se mantienen disponibles. Estado: en monitoreo preventivo. **Fuente: RNEC (Vigilancia Digital).**

Mediante verificación en fuentes abiertas se identificó en la red social X una publicación realizada el 21 de junio de 2026, a las 12:22 p.m., desde la cuenta verificada del Presidente de la República, Gustavo Petro (@petrogustavo), en la que se difunde un video de aproximadamente diez segundos, atribuido a un tercero, que haría referencia a la presunta existencia de votos pre marcados en la "mesa seis" del departamento del Atlántico. En el mensaje se solicita la atención de los testigos electorales, la impugnación de la mesa y la apertura de una investigación penal a los jurados de votación. Al momento de la verificación, la publicación registraba cerca de 54.300 visualizaciones. La valoración sustantiva del hecho —validez de la mesa, impugnación y eventual investigación penal— corresponde a las autoridades electorales y judiciales competentes (RNEC, CNE y Fiscalía); el PMU Ciber Electoral realiza el seguimiento de su dimensión digital (difusión, amplificación y eventual manipulación del contenido), sin pronunciarse sobre el fondo. **Fuente: CECIP – PONAL.**

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:

- Monitoreo permanente de la disponibilidad de los 36 portales (SOC RNEC), con bloqueo preventivo en firewall de red y WAF y mitigación automatizada de los intentos de DoS, sin afectación del servicio.
- Detección, bloqueo preventivo (sinkhole DNS) y reporte de abuso del dominio de suplantación; solicitud de comunicado oficial a la RNEC y revalidación pasiva periódica hasta el cierre.
- Seguimiento de direcciones IP maliciosas, dominios fraudulentos y cuentas de phishing, en articulación con la RNEC. y los ISP.
- Ciberpatrullaje en el marco del Plan Democracia (CECIP), con alertas remitidas, contenidos preventivos y preservación de publicaciones; remisión de casos a los entes judiciales cuando corresponde.
- Monitoreo preventivo del ecosistema de desinformación, con remisión de contenidos a la RNEC, el CNE y las plataformas para verificación, y articulación con las autoridades electorales y judiciales en los asuntos de su competencia.

SECCIÓN V — CONCLUSIÓN ESTRATÉGICA:

La jornada confirma una infraestructura electoral sólida y resiliente: disponibilidad total de los portales, mitigación automatizada de los ataques perimetrales y ausencia de incidentes cibernéticos. El vector de riesgo se concentra de manera definitiva en el entorno cognitivo, consolidando a la desinformación como la amenaza más crítica para la confianza en el proceso.

El punto de mayor atención es la narrativa que vincula una eventual indisponibilidad del portal con un supuesto "cambiazo" de resultados; dado el alto volumen de tráfico, cualquier latencia podría ser instrumentalizada como falsa evidencia de fraude. Por ello, la decisión estratégica debe orientarse a una comunicación de anticipación (*pre-bunking*): aclaraciones oficiales rápidas y visuales que expliquen los picos de demanda y reiteren la integridad del escrutinio, antes de que las narrativas se masifiquen.

En paralelo, se mantiene la postura preventiva sobre los incidentes puntuales —dominios de suplantación, IP maliciosas y phishing— con bloqueo y verificación continua hasta el cierre y la consolidación oficial de resultados por parte de la RNEC.