BOLETÍN PMU CENTRAL — Nro. [03] Segunda vuelta

Resumen ejecutivo

18 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	**6:00 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 presente boletín corresponde al corte del 18 de junio de 2026, a tres días de la Segunda Vuelta Presidencial del 21 de junio. A esta hora, el componente digital del proceso se mantiene estable y en observación: la infraestructura oficial de la Registraduría opera con normalidad, sin indisponibilidades ni afectaciones a la continuidad o integridad de los sistemas de votación y escrutinio.

La principal novedad del corte se concentra en un hallazgo, de una campaña masiva de infostealers de alcance global no aislado y fue reportado para las gestiones pertinentes; a la fecha no se confirman accesos efectivos. En los demás dominios —incidentes

gestionados, denuncias y evidencia digital, protección de sistemas y desinformación— no se registraron novedades en este corte.

El principal vector de riesgo permanece de carácter cognitivo y de identidad —suplantación, phishing dirigido al ciudadano y uso indebido de credenciales—, más que un compromiso directo del núcleo del proceso. El PMU Ciber Electoral mantiene el monitoreo y la respuesta interinstitucional coordinada de cara a la jornada del 21 de junio.

En el ámbito nacional y territorial, el CSIRT PONAL emitió una alerta preventiva sobre indicadores de compromiso de campañas de malware activas en el país (troyanos de acceso remoto), sin relación directa con la infraestructura electoral. Asimismo, se mantiene la gestión de los hallazgos de cortes anteriores: las exposiciones notificadas anteriormente, las aplicaciones móviles no oficiales fueron atribuidas y remitidas para gestión, y las narrativas de desinformación postelectoral continúan en revisión.

SECCIÓN III — SITUACIÓN POR DOMINIO.

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

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

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

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

El hallazgo evidencia un compromiso en la capa de identidad en infraestructura una campaña masiva de infostealers de alcance global y no de un evento aislado. Estado: notificado a la RNEC / en gestión**. Fuente: CCOCI.**

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

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

Análisis de sentimientos y clima narrativo en foros y redes

Categoría de Análisis	**Fuente / Metodología**	**Hallazgo Principal**	**Datos y Porcentajes**
Muestra Analizada	**eMonitor+**	Análisis de publicaciones en las plataformas Facebook y X.	**7.228** publicaciones priorizadas.

Clima General	**eMonitor+**	La señal dominante de la conversación es **negativa/hostil**.	**94%** clasificado como comunicación tóxica.
Desglose de Toxicidad	**eMonitor+**	Subcategorías dentro del universo de comunicación tóxica.	• Agresión verbal e insultos: **57,3%** • Comunicación polarizante: **26%** • Degradación/humillación: **16%**
Capa Cualitativa	**La Defensoría**	Seguimiento a la fase final del proceso en diferentes indicadores democráticos.	• Información veraz: **0%** • Lenguaje constructivo y eliminación de estigmatización: **16,7%** • Diálogo como compromiso democrático: **78,6%** *(Nivel alto)*
Foco Temático	**No especificada** *(Análisis de volumen)*	La conversación se centra en temas clave del país.	Seguridad/orden público, paz y corrupción.

Marcos Narrativos	**No especificada** *(Análisis de volumen)*	La agenda no está dominada solo por propaganda electoral, sino por emociones.	Marcos de amenaza, miedo, control territorial y legitimidad del proceso.

El monitoreo de fuentes abiertas evidencia un clima conversacional predominantemente hostil de cara a la jornada, con un amplio predominio de comunicación tóxica (agresión, polarización y degradación) y una agenda estructurada sobre marcos emocionales —amenaza, miedo, orden público y legitimidad del proceso— más que sobre el contraste programático. La etiqueta #Fraude se mantiene como la señal más sensible, asociada a narrativas de actas adulteradas y resultados anticipados, y el MinTIC advirtió la presencia de operaciones coordinadas de amplificación de narrativas. En contraste, la revisión de superficie de señales tipo "dark web" no halló confirmación abierta de filtraciones atribuidas en el periodo revisado. En consecuencia, el principal vector de riesgo en este frente es de carácter cognitivo y reputacional, con potencial de escalamiento postelectoral, sin que se evidencie un compromiso directo de la infraestructura electoral. Estado: en monitoreo / observación. **Fuente: Procuraduría (GPDAI).**

SECCIÓN IV — MEDIDAS DE PROTECCIÓN ADOPTADAS

Durante este corte, las instancias del PMU Ciber Electoral mantuvieron un esquema de protección activo y coordinado, con monitoreo permanente del componente digital electoral y vigilancia continua de los portales e infraestructura de la Registraduría a través de su Centro de Operaciones de Seguridad (SOC).

SECCIÓN V — CONCLUSIÓN ESTRATÉGICA:

A tres días de la Segunda Vuelta Presidencial, el componente digital del proceso se mantiene estable: la infraestructura oficial de la Registraduría opera con normalidad, sin indisponibilidades ni afectaciones a la integridad de los sistemas. El corte se caracteriza por el desplazamiento del riesgo hacia la capa de identidad, con la exposición de credenciales institucionales como vector más relevante.

Esta exposición no constituye un evento aislado, sino la manifestación local de una campaña global de infostealers; por ello, la prioridad inmediata es el restablecimiento de las credenciales afectadas, la revisión de las cuentas involucradas y el refuerzo de la autenticación multifactor, de manera que un compromiso en la capa de identidad no derive en accesos no autorizados a servicios asociados al proceso electoral. En paralelo, persisten las exposiciones notificadas al CNE —en proceso de corrección— y la gestión de narrativas de desinformación postelectoral orientadas a instalar miedo y pánico preventivo, que se mantienen en revisión por su potencial de amplificación.

En consecuencia, el riesgo más probable de cara al 21 de junio sigue siendo de carácter reputacional y cognitivo —degradación de la confianza, suplantación, phishing y uso indebido de credenciales dirigidos al ciudadano—, seguido del riesgo de orden público

posterior a los resultados, amplificado por desinformación; el riesgo de sabotaje directo al proceso permanece acotado por los controles existentes. La prioridad estratégica es doble: cerrar de forma prioritaria las exposiciones de identidad y las notificadas a las entidades (en especial las del CNE), y defender la confianza ciudadana en el proceso. El PMU Ciber Electoral mantiene una respuesta interinstitucional coordinada, preventiva y articulada, con monitoreo 24/7 hasta el cierre de la jornada.

SECCIÓN VII — GESTION NACIONAL Y TERRITORIAL

El CSIRT PONAL emitió una alerta (Boletín No. 39-2026, TLP:GREEN) sobre múltiples indicadores de compromiso asociados a campañas de malware activas en Colombia, que podrían afectar la confidencialidad, integridad y disponibilidad de la información. Las campañas distribuyen troyanos de acceso remoto (RAT) de las familias RemcosRAT, QuasarRAT y AsyncRAT, los cuales permiten a un atacante el control remoto del equipo, el robo de información y la ejecución de comandos. Los indicadores —servidores de comando y control (C2), dominios DNS maliciosos (principalmente sobre servicios de DNS dinámico como duckdns, ydns y dynu) y hashes SHA-256 de los archivos maliciosos, con fecha de corte 18 de junio de 2026— fueron documentados y compartidos con las instancias del PMU para su bloqueo y monitoreo preventivo. El hallazgo no se relaciona directamente con la infraestructura electoral y se reporta a título de alerta preventiva. Estado: en monitoreo preventivo. **Fuente: CSIRT PONAL.**