BOLETÍN PMU CENTRAL — Nro. [05] Segunda vuelta

Resumen ejecutivo

20 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

Al corte del 20 de junio de 2026, víspera de la segunda vuelta presidencial, el estado general del proceso se mantiene estable en observación, sin afectaciones a la disponibilidad de la infraestructura electoral. El SOC de la Registraduría reportó operación normal de sus portales y servicios durante las ventanas de monitoreo de la mañana (05:30–11:30 a.m.), con un incremento progresivo y esperable del tráfico —de 2.2 a 7.5 millones de solicitudes por corte— gestionado con normalidad y sin ataques de denegación de servicio (DoS) ni sobre el firewall de aplicaciones web (WAF). No se registraron incidentes de ciberseguridad.

En el frente de amenazas, el ColCERT y las instancias del PMU dieron tratamiento a casos de presunta exposición de datos personales asociados al ecosistema de la contienda electoral, notificados a los responsables del tratamiento y puestos en conocimiento de las autoridades competentes (Fiscalía y SIC), precisando en todos los casos el rol técnico —no judicial— del ColCERT y el carácter no verificado de la información obtenida en fuentes abiertas. Asimismo, el CSIRT Defensa reportó la exposición de credenciales institucionales de sistemas del CNE, reporte que fue puesto en conocimiento del CNE con recomendaciones de rotación inmediata y autenticación multifactor. De forma preventiva se emitió la alerta sobre la campaña global "FortiBleed" (abuso masivo de credenciales en dispositivos Fortinet) https://www.colcert.gov.co/800/w3-article-439118.html, no relacionada con la infraestructura electoral, pero con impacto en el sector público. En materia de desinformación, se mantienen en monitoreo varias narrativas y contenidos manipulados con inteligencia artificial, sin viralidad consolidada, ni alteración del normal desarrollo del proceso. La articulación interinstitucional del PMU Ciber Electoral permanece activa, con énfasis en la protección de la jornada.

SECCIÓN III — SITUACIÓN POR DOMINIO.

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

Durante la mañana del 20 de junio, el Centro de Operaciones de Seguridad (SOC) de la Registraduría Nacional del Estado Civil reportó operación estable de sus portales y servicios electorales, sin afectaciones a la disponibilidad. A lo largo de las ventanas de monitoreo (05:30–11:30 a.m.), el portal institucional de la Registraduría registró un incremento progresivo del tráfico —de 2.2 a 7.5 millones de solicitudes por corte—, gestionado con normalidad; los servicios de Descargas, Resultados y atención al ciudadano (SAC) operaron sin novedad. La nube segura bloqueó preventivamente los eventos detectados a nivel de firewall de red, y no se presentaron eventos ni ataques de tipo denegación de servicio (DoS) ni sobre el firewall de aplicaciones web (WAF). Estado: ESTABLE / sin novedad. **Fuente: RNEC (SOC).**

Informe N°4 — corte 09:30–11:30 a.m.

- registraduria.gov.co: 7.5 M solicitudes · 216 mil eventos bloqueados · sin DoS/WAF
- Descargas: 48.3 mil · 561 bloqueados
- Resultados: 498 mil · 8 mil bloqueados
- SAC: 8.8 mil · 28 bloqueados

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 ColCERT identificó, mediante monitoreo de fuentes abiertas, una muestra de registros de carácter personal disponible en un foro de la web profunda, atribuida a una base de datos de un movimiento político en el marco de la contienda electoral. El hallazgo se enmarca en una presunta exposición pública de dicha base, divulgada previamente por una

alianza periodística. Se precisa que el ColCERT no accedió a los sistemas, ni a la base del responsable: los registros observados corresponden únicamente a una muestra disponible públicamente en el foro —no a la base completa—, y su contenido específico permanece como información atribuida a fuentes abiertas, no verificada de manera independiente. Por la sensibilidad de la información y su potencial para habilitar fraude, suplantación de identidad y desinformación, el ColCERT notificó al responsable del tratamiento las recomendaciones de aseguramiento (Ley 1581 de 2012) y puso el caso en conocimiento de las autoridades competentes (Fiscalía General de la Nación y Superintendencia de Industria y Comercio) para las actuaciones que correspondan. La muestra se mantiene bajo reserva y a disposición de las autoridades por canal seguro. Estado: notificado / puesto en conocimiento / en gestión. **Fuente: ColCERT.**

La DIJIN, en articulación con el CSIRT PONAL, emitió una alerta de ciberseguridad relacionada con la identificación de una posible exfiltración de datos de la campaña de un candidato presidencial. El caso fue remitido al Área de Investigación Anticorrupción de la DIJIN y al CSIRT PONAL, que emitió la alerta correspondiente mediante su boletín #06. Estado: en investigación / en seguimiento. **Fuente: DIJIN / CSIRT PONAL.**

El ColCERT emitió la alerta AL-20260619-101 (TLP:CLEAR) sobre "FortiBleed" https://www.colcert.gov.co/800/w3-article-439118.html, una campaña global de abuso masivo de credenciales que compromete la seguridad perimetral de dispositivos Fortinet FortiGate. A diferencia de los ataques tradicionales, no explota una vulnerabilidad de software, sino el aprovechamiento de credenciales administrativas legítimas y de hashes criptográficos débiles que permanecen tras la actualización de los equipos. A escala global afecta a cerca de 73.900 dispositivos en 194 países; Colombia figura entre los países más afectados, con más de 2.400 interfaces de administración expuestas y afectación confirmada en 27 organizaciones, algunas del sector público. El riesgo incluye el control total del firewall, el monitoreo del tráfico cifrado (VPN), el salto hacia redes internas y la preparación de ataques de ransomware. La campaña no está relacionada con la infraestructura electoral; no obstante, por su impacto en el sector público se reporta como alerta preventiva. El ColCERT compartió con las instancias del PMU los indicadores y las recomendaciones de endurecimiento —deshabilitar la administración expuesta a Internet, restablecer credenciales con mayor complejidad, activar el doble factor de autenticación (MFA) de forma obligatoria, depurar los hashes débiles y enviar los registros a un sistema de monitoreo externo— y recomienda a las entidades con tecnología Fortinet, asumir como comprometidas sus credenciales actuales y aplicar la mitigación. Estado: alerta emitida / en monitoreo preventivo. **Fuente: ColCERT (AL-20260619-101).**

El CSIRT Defensa reportó un hallazgo crítico activo de exposición de credenciales institucionales del ecosistema del CNE, identificadas en canales de Telegram y foros de cibercrimen especializados en la venta de registros de robo de información (stealer logs). El CSIRT Defensa puso el hallazgo en conocimiento del CNE como acción prioritaria requerida, con recomendaciones de remediación: rotación inmediata de la credencial administrativa comprometida, autenticación multifactor (MFA) en los sistemas internos, revisión de los registros de acceso para descartar uso indebido y monitoreo continuo de exposición de credenciales institucionales durante el resto del periodo electoral. Estado: notificado al CNE / acción prioritaria requerida / en gestión. **Fuente: CSIRT Defensa.**

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

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

Durante el corte se mantiene activo el monitoreo del ecosistema de desinformación electoral, señalado por diversas fuentes como el principal factor de riesgo de la recta final. De acuerdo con el monitoreo de la Procuraduría (GPDAI) y de la observación electoral (MOE–PNUD), persisten narrativas de fraude sin evidencia sólida, montajes audiovisuales y piezas alteradas con inteligencia artificial —incluidos deepfakes—, junto con un clima de conversación digital marcadamente hostil hacia candidaturas, periodistas y autoridades electorales. El segundo informe eMonitor+ (MOE–PNUD) reportó un alto componente de comunicación tóxica en la muestra priorizada de publicaciones analizadas (95,3%).

En el plano de la verificación, la MOE y verificadores independientes —entre ellos EFE Verifica— desmintieron varias narrativas en circulación, relacionadas, entre otras, con supuestas irregularidades en formularios E-14 y afirmaciones inventadas atribuidas a las campañas. En el monitoreo de fuentes abiertas se observan, además, etiquetas de alta sensibilidad reputacional asociadas a sospechas de fraude, así como nichos hacktivistas de baja tracción pública verificable. **Fuente: GPDAI–Procuraduría**

SECCIÓN IV — MEDIDAS DE PROTECCIÓN ADOPTADAS

Durante este corte, las instancias del PMU Ciber Electoral mantuvieron un esquema de monitoreo y respuesta articulado para proteger la infraestructura y el ecosistema digital del proceso. Entre las medidas adoptadas se destacan:

- Monitoreo permanente de la disponibilidad de los portales y servicios electorales (SOC de la RNEC), con bloqueo preventivo de eventos a nivel de firewall de red.
- Notificación a los responsables del tratamiento y puesta en conocimiento de las autoridades competentes (Fiscalía y SIC) de los casos de presunta exposición de datos personales, con reserva y trazabilidad de la información.
- Notificación al CNE de la exposición de credenciales institucionales, revisión de los registros de acceso y monitoreo continuo de exposición de credenciales.
- Difusión a las instancias del PMU de los indicadores de compromiso (IoC) y de las recomendaciones de endurecimiento de las alertas vigentes —incluida la alerta preventiva "FortiBleed"—, y refuerzo de credenciales y MFA en las cuentas institucionales afectadas.
- Monitoreo preventivo de narrativas de desinformación y contenidos manipulados con IA, con articulación para verificación y, cuando corresponde, reporte a plataformas.

SECCIÓN V — CONCLUSIÓN ESTRATÉGICA:

Al cierre de este corte, en la víspera de la segunda vuelta presidencial, el balance de ciberseguridad del proceso es estable: la infraestructura electoral opera con normalidad y sin afectaciones a la disponibilidad, y no se han materializado incidentes que comprometan el desarrollo de la jornada. El panorama de riesgo se concentra en la exposición y posible uso indebido de datos personales y de credenciales institucionales, la suplantación de la identidad institucional (dominios y bots fraudulentos) y la circulación de

narrativas de desinformación y contenidos manipulados con IA, fenómenos que se mantienen bajo monitoreo y gestión sin escalamiento al corte.

De cara a la jornada del 21 de junio, se recomienda sostener el monitoreo reforzado de la disponibilidad y de los intentos de suplantación, impulsar la rotación de credenciales comprometidas y la activación de autenticación multifactor, mantener la articulación interinstitucional para la verificación y respuesta ágil ante la desinformación, y reiterar a las entidades —en especial las que cuentan con tecnología Fortinet— la aplicación inmediata de las medidas de endurecimiento frente a la campaña FortiBleed. El ColCERT, en su rol de Secretaría Técnica, mantiene activa la coordinación del PMU Ciber Electoral para la protección integral del proceso.