BOLETÍN PMU CENTRAL — Nro. [01] Segunda vuelta Presidencial

Resumen ejecutivo

16 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.**

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 primer corte del PMU Ciber Electoral 2026 de cara a la Segunda Vuelta Presidencial del 21 de junio de 2026*. A esta hora, el componente digital se mantiene estable: de acuerdo con el reporte del SOC de la Registraduría no se presentaron indisponibilidades en los portales web, y la infraestructura electoral conserva una alta resiliencia operativa, con navegación fluida para la ciudadanía y sin afectaciones a la continuidad ni a la integridad de los sistemas.

En materia de desinformación se atiende un ecosistema activo y persistente: se documentaron una encuesta falsa atribuida a INVAMER (ya desmentida), la difusión de supuestos tarjetones marcados en consulados y un patrón más amplio de narrativas de fraude, falsas encuestas y piezas alteradas con inteligencia artificial (deepfakes), sin que se haya configurado una campaña con impacto determinante sobre el proceso. En este escenario, el principal vector de riesgo es de carácter reputacional y cognitivo, la manipulación de la percepción ciudadana más que un compromiso directo de la infraestructura.

El PMU Ciber Electoral mantiene su rol de monitoreo, anticipación y respuesta interinstitucional coordinada, y dará continuidad al seguimiento durante los días previos y la jornada del 21 de junio para asegurar una respuesta oportuna ante cualquier eventualidad.

SECCIÓN III — SITUACIÓN POR DOMINIO.

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

De acuerdo con el reporte del Centro de Operaciones de Seguridad (SOC) de la Registraduría Nacional del Estado Civil, correspondiente al periodo comprendido entre las 00:00 y las 18:00 horas del 16 de junio de 2026, no se presentaron indisponibilidades en los portales web. *La infraestructura tecnológica del componente electoral mantiene una alta resiliencia operativa:* las plataformas operan con normalidad y los niveles de tráfico se conservan dentro de los umbrales esperados, permitiendo una navegación fluida para la ciudadanía. No se identificaron afectaciones, interrupciones ni anomalías que comprometan la continuidad o la integridad de los sistemas, lo que confirma la estabilidad del componente digital en esta fase del proceso. La infraestructura permanece bajo seguimiento permanente de cara a la jornada del 21 de junio.

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**):**

Se reportó un posible hallazgo crítico asociado a un dominio externo que aloja un portal de consulta electoral y que, según el reporte, realizaría consultas y redireccionamientos hacia un portal legítimo. De acuerdo con el análisis remitido, el portal externo presentaría vulnerabilidades de seguridad potencialmente explotables, lo que configuraría un escenario de alta criticidad.

El ColCERT adelanta la validación del hallazgo para determinar si este portal es un activo autorizado de la entidad o un dominio no autorizado que opera con acceso indebido

a sistemas institucionales. Una vez confirmada su naturaleza, se adoptarán las acciones que correspondan: verificación de la legitimidad del dominio y bloqueo preventivo de la dirección IP asociada, notificación a la entidad y, de confirmarse acceso no autorizado, aislamiento del recurso. Estado: en validación. **Fuente: CSIRT Defensa.**

Se identificó una campaña de aplicaciones móviles Android fraudulentas que suplantan los servicios electorales más consultados por la ciudadanía ("consulte su lugar de votación" y "cédula digital"), distribuidas por fuera de las tiendas oficiales (tiendas de terceros y, probablemente, cadenas de WhatsApp y SMS). El análisis del ColCERT evidenció un perfil de riesgo alto, con comportamiento de phishing móvil y de rastreo del usuario (adware) y que, pese a no presentar detecciones en los motores antivirus, facilita su instalación desprevenida. Por el alto volumen de ciudadanos que consultará estos servicios en los días previos al 21 de junio, se recomienda coordinar con la Registraduría la emisión de un comunicado oficial que precise los únicos canales válidos de consulta (la aplicación oficial en Google Play y el portal registraduria.gov.co); entretanto, se mantiene el monitoreo y la gestión para su retiro. Estado: en monitoreo y gestión de retiro. **Fuente: ColCERT.**

Se emitió una alerta de ciberseguridad sobre campañas de malware activas en Colombia, distribuidas mediante una falsa notificación que suplanta a la Fiscalía General de la Nación como señuelo. La alerta caracterizó múltiples indicadores de compromiso 13 familias de malware y 134 archivos maliciosos documentados y compartidos para su monitoreo, prevención y gestión oportuna. Estas amenazas buscan comprometer la confidencialidad, la integridad y la disponibilidad de la información; tras el análisis, el nivel de riesgo asociado se clasifica como mínimo. Estado: en monitoreo preventivo. **Fuente: CSIRT PONAL.**

5. **D5 — Protección de sistemas:**

En el marco del Programa de Corresponsabilidad para los Procesos Electorales, se realizó análisis de superficie de ataque y gestión de vulnerabilidades sobre la infraestructura web del Consejo Nacional Electoral (CNE) y de la Registraduría Nacional del Estado Civil (RNEC). En ambas entidades la postura de seguridad es adecuada: no se identificaron vulnerabilidades críticas ni altas. En el CNE, de los sitios evaluados, se halló un único punto de severidad media ya notificado para su corrección junto con recomendaciones de endurecimiento preventivo, En la RNEC, los hallazgos son de carácter informativo, sin afectación a la operación. Las recomendaciones de hardening fueron remitidas a las entidades como medida preventiva de cara a la jornada del 21 de junio. Estado: notificado / en hardening preventivo. **Fuente: ColCERT.**

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

A través de componentes de inteligencia de amenazas se identificó la circulación en redes sociales (X, Facebook e Instagram) de una imagen falsa atribuida a la firma encuestadora INVAMER oficialmente el contenido el 15 de junio de 2026. El caso corresponde a una operación de desinformación electoral orientada a manipular la percepción del electorado en los días previos a la votación. Se mantiene el monitoreo de su propagación y se alertó a los equipos de comunicaciones institucionales sobre este patrón de suplantación de encuestadoras. Estado: en monitoreo. **Fuente: ColCERT.**

Se reportó la circulación de videos e imágenes que afirman la existencia de tarjetones supuestamente marcados de manera anticipada a favor de uno de los candidatos en consulados del exterior principalmente Londres y Bolivia, presentados como presunta evidencia de fraude electoral. El contenido se difunde principalmente en X, TikTok y Facebook, con lenguaje alarmista y llamados a denunciar, buscando generar desconfianza sobre el voto en el exterior y desprestigiar a las autoridades electorales. El monitoreo evidenció alta capacidad de viralización, impulsada por cuentas de alta influencia y posibles redes de amplificación coordinada. Se recomienda articular la verificación con la Registraduría y el CNE, y contrarrestar con mensajes oficiales que aclaren el origen y la validez de los tarjetones. Estado: en revisión / reporte a plataformas. **Fuente: CCOCI.**

El Grupo de Protección de Datos y Activos de Información (GPDAI) de la Procuraduría, con base en monitoreo de fuentes abiertas, documentó un ecosistema de desinformación electoral activo y persistente, clasificado como de riesgo alto. El patrón más recurrente combina narrativas falsas sobre supuesto fraude, falsas encuestas, comunicados apócrifos atribuidos a grupos armados, videos antiguos recontextualizados, imágenes sacadas de contexto y piezas alteradas con inteligencia artificial (deepfakes), difundidas principalmente en X, Facebook, Instagram, TikTok y WhatsApp. Verificadores independientes (ColombiaCheck y EFE Verifica) desmintieron varias de estas piezas. Estado: en monitoreo. **Fuente: GPDAI – Procuraduría.**

SECCIÓN IV — MEDIDAS DE PROTECCIÓN ADOPTADAS

Durante este corte, las instancias del PMU Ciber Electoral mantuvieron un esquema de protección activo y coordinado. Se sostiene el monitoreo permanente del componente digital electoral, incluida la vigilancia continua de los portales e infraestructura de la Registraduría a través de su Centro de Operaciones de Seguridad (SOC). Frente al dominio externo asociado a sitios legítimos, se adelanta su verificación y validación con la entidad, con bloqueo preventivo de la dirección asociada y aislamiento en caso de confirmarse un acceso no autorizado. Respecto a las aplicaciones móviles fraudulentas que suplantan servicios de la Registraduría, se mantiene la gestión y se coordina con la entidad la emisión de un comunicado oficial que precise a la ciudadanía los únicos canales válidos de consulta.

En cuanto a las amenazas de malware y phishing, los indicadores de compromiso fueron documentados y compartidos con las instancias para su bloqueo y monitoreo preventivo y subidos a la plataforma de datos abiertos de MINTIC. En materia de protección de sistemas, se realizó análisis de superficie de ataque y gestión de vulnerabilidades sobre la infraestructura del CNE y la RNEC, remitiendo a las entidades las recomendaciones de endurecimiento (hardening) como medida preventiva. En el plano informativo, se alertó a

los equipos de comunicaciones institucionales sobre los patrones de desinformación y suplantación detectados, articulando la verificación de contenidos con la Registraduría y el CNE y su reporte a las plataformas digitales.

El PMU mantiene la respuesta interinstitucional coordinada y el monitoreo 24/7 de cara a la jornada del 21 de junio.

SECCIÓN V — CONCLUSIÓN ESTRATÉGICA:

El panorama de amenazas de cara a la Segunda Vuelta Presidencial 2006 muestra una superficie activa de carácter multivector, orientada a manipular y explotar el proceso electoral más que a comprometer directamente su infraestructura. En el plano informativo, mediante campañas de desinformación (encuesta falsa atribuida a INVAMER, supuestos tarjetones marcados en consulados y narrativas de fraude y deepfakes documentadas por la Procuraduría); y en el plano técnico, mediante suplantación: aplicaciones móviles fraudulentas que imitan servicios y un dominio externo que consulta el portal legítimo. Esta convergencia sugiere un ecosistema que busca erosionar la confianza ciudadana y aprovechar la alta demanda de servicios electorales en los días previos a la jornada.

En síntesis, el componente digital del proceso permanece estable; la prioridad estratégica no es solo defender la infraestructura, sino defender la confianza ciudadana en el proceso, frente a lo cual el PMU mantiene una respuesta coordinada, preventiva y articulada entre las instancias de cara al 21 de junio.

En el entorno de orden público, se registraron pronunciamientos de actores armados ilegales declarando su no interferencia en la jornada electoral, incluido un cese al fuego unilateral anunciado para los días cercanos a los comicios. Estas declaraciones tienen un efecto estabilizador en el discurso público, aunque no eliminan por sí mismas el riesgo operacional en algunas zonas del territorio, por lo que el panorama se mantiene bajo seguimiento permanente por la fuerza pública.