## BOLETÍN PMU CENTRAL — Nro. [02] Segunda vuelta

# Resumen ejecutivo

17 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 17 de junio de 2026 de cara a la Segunda Vuelta Presidencial del 21 de junio. A esta hora, el componente digital se mantiene estable: la infraestructura oficial de la Registraduría opera con normalidad, sin indisponibilidades ni afectaciones a la continuidad o integridad de los sistemas.

En el plano de riesgos se identificaron intentos de suplantación de comunicaciones oficiales, enlaces externos relacionados con servicios electorales que requieren seguimiento preventivo y la indisponibilidad de una plataforma de apoyo al proceso electoral, situación ya informada a la entidad correspondiente. En materia de protección, se remitieron recomendaciones preventivas a las campañas que avanzan a la segunda

vuelta y se notificaron hallazgos relevantes a las entidades responsables para su atención oportuna.

En materia de desinformación se atienden narrativas del escenario postelectoral orientadas a instalar miedo y pánico preventivo —advertencias de violencia tras los resultados y llamados a abastecerse—, con indicios de amplificación coordinada y sin que se haya configurado una afectación determinante sobre el proceso. El principal vector de riesgo permanece de carácter reputacional y cognitivo —la manipulación de la percepción ciudadana— más que un compromiso directo de la infraestructura. El PMU Ciber Electoral mantiene el monitoreo y la respuesta interinstitucional coordinada de cara a la jornada del 21 de junio.

**SECCIÓN III — SITUACIÓN POR DOMINIO**.

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

De acuerdo con el SOC de la Registraduría Nacional del Estado Civil, en el periodo comprendido entre las 17:00 del 16 de junio y las 17:00 del 17 de junio de 2026 no se presentaron indisponibilidades en los portales web. La infraestructura opera con normalidad, sin afectaciones a la continuidad ni a la integridad de los sistemas. Estado: estable. **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**):**

Se identificaron intentos de suplantación asociados al proceso electoral, por lo que se activaron acciones de seguimiento y prevención en coordinación con las instancias competentes. Estado: en monitoreo preventivo. **Fuente: RNEC.**

El equipo de ColCERT adelantó una revisión preventiva de enlaces asociados a servicios web relacionados con las elecciones presidenciales. Como resultado, se confirmó el funcionamiento adecuado de los canales oficiales y se identificaron algunos enlaces externos que, aunque dirigen a información institucional, requieren seguimiento y monitoreo para reducir riesgos de confusión o uso indebido por parte de terceros. **Fuente: ColCERT.**

ColCERT identificó una indisponibilidad en una plataforma de apoyo al proceso electoral. La situación fue informada oportunamente a la entidad correspondiente para su validación y atención, y se mantienen acciones de seguimiento preventivo para reducir posibles riesgos asociados y orientar a la ciudadanía hacia canales oficiales de información. **Fuente: ColCERT.**

**5. D5 — Protección de sistemas:**

ColCERT realizó análisis preventivo de exposición digital sobre los portales web de las campañas que avanzan a la segunda vuelta, usando únicamente información pública y sin interactuar con los sistemas. En ambos casos se identificaron oportunidades de fortalecimiento. No se identificaron ataques en curso, accesos comprometidos ni afectación al normal desarrollo del proceso. Los hallazgos fueron remitidos a cada campaña con recomendaciones de corrección. **Fuente: ColCERT.**

El CSIRT Defensa identificó aspectos de seguridad que requerían fortalecimiento en un sistema institucional asociado al proceso electoral. La información fue confirmada y comunicada a la entidad correspondiente para su atención prioritaria, y actualmente se adelantan las acciones necesarias para reforzar las medidas de protección. Estado: notificado a la entidad / en corrección. **Fuente: CSIRT Defensa.**

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

A través del monitoreo de fuentes abiertas se identificó la circulación de una narrativa alarmista de cara al escenario postelectoral que, reencuadrando declaraciones de dirigentes políticos sobre posibles movilizaciones ciudadanas según el resultado de la segunda vuelta, afirma que "se va a incendiar el país". El contenido se difunde principalmente en Facebook y X mediante piezas gráficas y publicaciones con versiones contradictorias entre sí, y busca generar miedo, polarización y la percepción de una eventual violencia organizada. Hasta el momento no se identifica evidencia de una instrucción coordinada para generar desórdenes ni una infracción directa, por lo que se mantiene en observación por su potencial de amplificación y de afectación a la confianza ciudadana; la dimensión de orden público se articula con las autoridades competentes. Estado: en revisión. **Fuente: CCOCI.**

Se identificó igualmente una narrativa de "estallido social 2.0" que advierte sobre supuestos bloqueos viales, protestas masivas y afectaciones al abastecimiento tras los resultados, acompañada de llamados a la ciudadanía a abastecerse de alimentos y productos básicos. El contenido circula en Facebook, X y mensajería, y se observa un mismo texto replicado de forma idéntica en varias cuentas, incluida al menos una rotulada como extranjera, lo que sugiere un patrón de amplificación coordinada. Hasta el momento no existe ninguna alerta oficial de desabastecimiento o bloqueo generalizado. Se recomienda la validación con las autoridades competentes para prevenir la amplificación de rumores. Estado: en revisión. **Fuente: CCOCI.**

En el marco del monitoreo de desinformación digital, una publicación en la red social X que se viene utilizando técnica de deepfake conocida como Face Swap (intercambio de rostros) con el objetivo de engañar a la ciudadanía. La amenaza consiste en la difusión de un video manipulado mediante Inteligencia Artificial, donde se suplanta la identidad del candidato Iván Cepeda. Para lograr una apariencia legítima, los atacantes sincronizaron de manera precisa los movimientos de los labios del video con una pista de audio generada a partir de un modelo de voz entrenado con la IA del candidato, potenciando el alcance y la credibilidad del engaño. **Fuente: CECIP.**

**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). Frente a los riesgos identificados, se activaron medidas preventivas de seguimiento, coordinación interinstitucional y fortalecimiento de la capacidad de respuesta.

En relación con los servicios electorales más consultados, se adelantan acciones de verificación de canales oficiales, seguimiento preventivo de enlaces externos y coordinación con las entidades responsables para fortalecer la orientación a la ciudadanía y reducir riesgos de confusión.

En materia de protección de sistemas, se remitieron recomendaciones preventivas a las entidades y campañas analizadas para fortalecer sus medidas de seguridad. En el plano informativo, se alertó a los equipos de comunicaciones institucionales sobre los contenidos de desinformación detectados, articulando con las autoridades competentes la verificación de información y, cuando corresponde, 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:**

A cuatro 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. No obstante, el corte evidencia una superficie de amenazas activa que abarca varios frentes, orientada principalmente a explotar la confianza ciudadana y la alta demanda de servicios electorales, más que a comprometer directamente el núcleo del proceso.

En el plano digital se observan distintos frentes de atención, principalmente orientados a la suplantación de comunicaciones, la circulación de enlaces externos relacionados con servicios de interés ciudadano y algunas situaciones operativas ya informadas a las entidades responsables. En el plano informativo persisten narrativas postelectorales que pueden generar preocupación y afectar la percepción pública. Aunque estos hechos se presentan de manera concurrente, continúan siendo atendidos bajo seguimiento institucional y coordinación preventiva.

En consecuencia, el principal reto de cara al 21 de junio sigue concentrado en la protección de la confianza ciudadana frente a intentos de suplantación, rumores y contenidos engañosos, más que en afectaciones directas a la infraestructura del proceso. La prioridad

estratégica es fortalecer las medidas preventivas, acompañar a las entidades responsables en la atención de hallazgos y mantener una comunicación clara hacia la ciudadanía. El PMU Ciber Electoral mantiene una respuesta interinstitucional coordinada y preventiva hasta el cierre de la jornada.

## SECCIÓN VI — SEGUIMIENTO A CORTES ANTERIORES

*(Corte anterior: Boletín 01 — 16/06/2026, 6:00 p.m.)*

| **Situación reportada en corte anterior** | **Qué se hizo** | **Estado actual** |
|---|---|---|
| Sitio externo relacionado con un servicio de consulta electoral cuya legitimidad fue revisada por la entidad competente. | La entidad informó que la situación corresponde a un enlace externo que ya se encuentra en proceso de ajuste dentro de su entorno oficial. Se mantienen las acciones de verificación y seguimiento hasta confirmar el cierre de la gestión. | **En gestión** *(se adelanta el retiro del redireccionamiento; pasa a Neutralizada/Cerrada una vez confirmado el cierre)* |
| Aplicaciones móviles falsas que suplantaban servicios de la Registraduría (consulta de lugar de votación y cédula digital). | Se informo a la RNEC para las coordinaciones respectivas para el retiro de las aplicaciones falsas, se le recomienda sacar un comunicado para informar a la ciudadanía cuáles son los únicos canales oficiales de consulta. | **En gestión:** *Pendiente confirmación acciones* |
| **Contenido fraudulento que suplantaba comunicaciones institucionales para inducir a error a la ciudadanía.** | Se documentaron y compartieron las señales de la amenaza con las entidades para su bloqueo y vigilancia preventiva. El riesgo se mantiene bajo. | **En seguimiento:** *Pendiente confirmación acciones* |
| Revisión preventiva de la seguridad de los sistemas web del CNE y la Registraduría. | Se entregaron a ambas entidades las recomendaciones para reforzar la seguridad de sus sitios antes de la jornada. (Gestión de Vulnerabilidades y Recomendaciones) | **En gestión** *Pendiente confirmación acciones* |
| Imagen falsa de una encuesta atribuida a Invamer sobre los resultados de la segunda vuelta. | Se confirmó que era falsa —la firma la desmintió el 15 de junio— y se alertó a los equipos de comunicaciones. Se mantiene la vigilancia de su difusión. | **En seguimiento:** *Pendiente confirmación acciones* |
| Videos que afirmaban la existencia de tarjetones | Se coordinó la verificación con la Registraduría y el CNE y se | **En gestión:** *Pendiente confirmación acciones* |

| Situación reportada en corte anterior | Qué se hizo | Estado actual |
|---|---|---|
| marcados de manera anticipada en consulados del exterior. | reportó el contenido a las plataformas digitales para su revisión. | |
| Conjunto general de desinformación electoral (rumores de fraude, encuestas falsas y contenidos alterados con inteligencia artificial). | Se mantiene el monitoreo del conjunto de contenidos; varios fueron desmentidos por verificadores independientes. | **En seguimiento** |