## BOLETÍN PMU Ciber Electoral — Nro. [001] – [11:00 p.m.]

### SECCIÓN I — ESTADO GENERAL DE LA JORNADA

| | |
|---|---|
| **Indicador** | **ESTABLE** |
| **Entidad Reportante** | PMU Ciber Electoral 2026 – Elecciones Presidenciales |
| **Hora del corte** | **11:00 p.m.** |

### SECCIÓN II — RESUMEN EJECUTIVO

Con corte a las *11:00 p.m. del 30 de mayo de 2026*, en preparación del inicio de la jornada de elecciones, el componente digital del proceso electoral presidencial se mantiene estable, bajo vigilancia permanente y sin afectaciones que comprometan la continuidad de la jornada. Las amenazas detectadas se encuentran identificadas y en seguimiento, sin impacto confirmado sobre la integridad del proceso. El PMU Ciber Electoral mantiene activas sus capacidades de monitoreo y articulación entre entidades, y dará continuidad al seguimiento durante el desarrollo de la jornada.

### SECCIÓN III — SITUACIÓN POR DOMINIO (DX).

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

La infraestructura tecnológica del componente electoral presenta una alta resiliencia operativa. Los niveles de tráfico se mantienen dentro de los umbrales de seguridad, permitiendo una navegación fluida para la ciudadanía.

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

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

El Centro Cibernético Policial mantiene el monitoreo permanente de redes sociales y canales abiertos durante la jornada, cubriendo los activos digitales de las entidades electorales (CNE y Registraduría) y del sector, con un alcance potencial superior a *30.000 millones de interacciones.*

La conversación electoral se desarrolla con normalidad, marcada por tendencias de apoyo y oposición propias del debate político. En el periodo se remitieron cuatro alertas y se preservó una publicación. Se hace seguimiento a denuncias ciudadanas que se encuentran en verificación —presuntas irregularidades sobre formularios E14,

suplantación de identidad electoral en el exterior y contenido sobre un candidato presidencial bajo verificación judicial—, así como

al normal desarrollo del plan de auditorías de la Registraduría y a los despliegues de seguridad del Plan Democracia.
Todo el material se encuentra en monitoreo, sin afectaciones confirmadas a la integridad del proceso.

4. **D4 — Amenazas identificadas - (**Fuente ColCERT, CCOCI, CECIP, DIPOL**):**

- **Suplantación al CNE (alta atención):** campaña activa de correos fraudulentos que engañan a la ciudadanía con una falsa designación como jurado de votación. En gestión para bloqueo y notificación a las autoridades electorales.
- **Sitios que imitan a la Registraduría (preventivo):** se detectaron páginas de creación reciente que copian el nombre de la entidad; remitidas a la Registraduría para verificación y bloqueo.
- **Posible exposición de datos de acceso (preventivo):** se identificaron pares de usuario y contraseña asociados a dos plataformas del Estado; las entidades fueron notificadas para su validación y las acciones de remediación necesarias.
- **Actividad del actor:** Se reporta actividad confirmada de un actor de perfil hacktivista, cuyo objetivo es generar impacto mediático en el contexto electoral. El actor afirma haber obtenido información de bases de datos de entidades del Estado —en particular de la Registraduría—, sin que exista, hasta el momento, confirmación técnica de un compromiso real de los sistemas; la entidad ya fue notificada y se adelanta la validación técnica correspondiente.
- **Verificación de la supuesta exposición de bases de datos de entidades del Estado:** Ante la circulación en redes y la alta difusión mediática de la supuesta exfiltración de bases de datos del Estado en el contexto electoral, ColCERT —como Secretaría Técnica del PMU Ciber Electoral— remitió a cada entidad presuntamente referida el reporte de situación, para su validación interna y la determinación de una posible afectación. De manera preliminar, las entidades que han respondido coinciden en que la información corresponde a datos previamente expuestos y, en algunos casos, de carácter público, sin evidencia de una vulneración nueva ni simultánea. *Estado: en validación por las entidades.*
- **Publicación del actor contra el CNE:** El actor difundió material atribuido al Consejo Nacional Electoral, incluyendo documentos y credenciales. La verificación indica que la información corresponde a una exfiltración previa —credenciales de 2023 y registros de usuarios de 2021 y 2022—, hecho confirmado por el propio CNE. No se trata de una vulneración nueva ni ocurrida durante la jornada; la divulgación busca impacto mediático en el contexto electoral. Fuentes: Policía Nacional, CCOCI y ColCERT.

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

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

**Se monitorean tres narrativas de desinformación dirigidas a sembrar dudas sobre la integridad del proceso:** una sobre supuestos ataques cibernéticos al sistema electoral, otra que exagera falsamente el número de votantes en el exterior (desmentida por la Registraduría) y una tercera, que cuestiona la custodia del software de escrutinio. *Ninguna corresponde a hechos confirmados*, se trata de contenido en monitoreo y verificación, sin afectación comprobada a la integridad del proceso electoral. Las entidades competentes están informadas y el PMU mantiene el seguimiento.

## SECCIÓN IV — MEDIDAS DE PROTECCIÓN ADOPTADAS

Las medidas de protección vigentes se mantienen sin cambios.

## SECCIÓN V — CONCLUSIÓN ESTRATÉGICA

Con corte a las *11:00 p.m. del 30 de mayo de 2026*, iniciando la jornada de elecciones, el entorno digital del proceso electoral presidencial se mantiene estable, bajo vigilancia permanente y sin afectaciones que comprometan la continuidad operativa de la jornada. *Las capacidades de monitoreo, seguimiento y articulación interinstitucional continúan activas, permitiendo mantener vigilancia preventiva sobre los riesgos asociados al entorno digital electoral.*

## SECCIÓN VI — SEGUIMIENTO A CORTES ANTERIORES

| Situación | Acción | Estado actual |
|---|---|---|
| Campaña suplanta al Consejo Nacional Electoral (CNE), utilizando como pretexto la "Designación Oficial como Jurado de Votación" para la jornada electoral. | [X] Bloqueo de IP<br>[X]Takedown de dominio<br>[X ] Notificación a RNEC<br>[X ] Notificación a CNE | Bloqueado |
| Hallazgo confirmado de actividad maliciosa del actor, con evidencia de recopilación, posible exposición y difusión de información estructurada de entidades gubernamentales (validado vía OSINT y correlación en Telegram/Discord/redes sociales). | ☑ Notificación a RNEC<br>☑ Otra: validación técnica interna de la supuesta exposición de bases de datos y verificación de integridad de la información institucional. | En Proceso |