

INFORME CONCLUSIVO DE ETHICAL HACKING

CLIENTE: Órgano Electoral Plurinacional - OEP

**REFERENCIA: INFORME CONCLUSIVO ELECCIONES
GENERALES 2025 2DA VUELTA**

Fecha: 26/10/25

Elaborado por: I-Quattro – División de Ciberseguridad

Índice

INDICACIONES DEL DOCUMENTO.....	1
Información Importante	1
EQUIPO DE TRABAJO	2
RESUMEN EJECUTIVO	3

INDICACIONES DEL DOCUMENTO

Información Importante

El presente informe ha sido elaborado en el marco de la evaluación de seguridad informática de los sistemas utilizados en la 2da Vuelta de las Elecciones Generales 2025.

Su contenido expone, de manera general y no técnica, los resultados alcanzados durante el proceso de evaluación, con el objetivo de dar a conocer el nivel de seguridad y confiabilidad de la plataforma informática empleada.

Este documento está destinado a fines informativos y de transparencia institucional, y no incluye información técnica detallada que pudiera comprometer la seguridad de la infraestructura evaluada.

EQUIPO DE TRABAJO

Para cualquier consulta sobre el contenido de este documento o de las pruebas realizadas, usted puede contactar a los consultores que trabajaron directamente en la actividad.

PROJECT MANAGER

IVAR BUEZO

ivar@i-quattro.com

PROJECT LEADER

ARIEL GUZMAN

ariel@i-quattro.com

PENTESTER

FRANZ ALVIS

franz@i-quattro.com

RESUMEN EJECUTIVO

En el marco del fortalecimiento de la seguridad tecnológica del **Órgano Electoral Plurinacional (OEP)** y en cumplimiento de su compromiso con la transparencia, integridad y confianza del proceso electoral presidencial – Segunda Vuelta 2025, el equipo consultor de **I-Quattro** llevó a cabo un acompañamiento técnico especializado orientado a la **verificación de la efectividad de las medidas de seguridad implementadas** en las plataformas críticas utilizadas durante el proceso.

Este trabajo dio continuidad a las acciones de remediación previamente desarrolladas, e incluyó la revisión técnica de las principales aplicaciones, infraestructuras y servicios tecnológicos de OEP, tanto en su entorno interno como en los servicios expuestos a internet.

El análisis contempló la ejecución de **pruebas de verificación (retest)** sobre los hallazgos reportados en evaluaciones anteriores, así como la validación de los controles de seguridad adoptados. De igual forma, se realizaron pruebas de penetración complementarias, internas y externas, con el fin de confirmar la efectividad de las medidas correctivas aplicadas y asegurar el cumplimiento de los estándares de seguridad requeridos para un proceso electoral de alta criticidad.

En la infraestructura interna, se constató que el OEP mantiene **controles de seguridad relevantes y vigentes**, tales como la segmentación de redes dedicadas al cómputo electoral, mecanismos de gestión de configuraciones y parches, protección antivirus en los equipos, discos duros cifrados y una adecuada gestión de usuarios y privilegios. Estas medidas contribuyen directamente a la mitigación de riesgos y al aseguramiento de la operación continua de los sistemas.

Como resultado de este acompañamiento, se verificó que las aplicaciones **SIREPRE** y **SCORC** sistemas centrales del proceso de transmisión y consolidación de resultados **mantuvieron un estado de seguridad adecuado previo y durante el proceso electoral**, sin evidenciar vulnerabilidades que pudieran afectar su funcionamiento o comprometer la información gestionada.

Las pruebas realizadas confirmaron que las **medidas implementadas fueron efectivas para garantizar la integridad, disponibilidad y confidencialidad de los datos**, asegurando así la estabilidad, confiabilidad y protección de las plataformas a lo largo de todo el proceso electoral.

En conclusión, el proceso electoral presidencial – Segunda Vuelta 2025 se desarrolló sobre **una infraestructura tecnológica segura, monitoreada y resiliente**, que permitió el funcionamiento correcto de los sistemas informáticos sin incidentes de seguridad reportados, reforzando la confianza en la transparencia y legitimidad de los resultados.

