

INFORME FINAL

**AUDITORÍA AL SISTEMA INFORMÁTICO
Y A LA INFRAESTRUCTURA TECNOLÓGICA
DEL PROGRAMA DE RESULTADOS ELECTORALES
PRELIMINARES (PREP)**

**PROCESO ELECTORAL LOCAL ORDINARIO 2017 – 2018
ESTADO DE OAXACA.**

28 de junio de 2018

Contenido

I. Resumen General	3
II. Desarrollo de la Auditoría	4
III. Resultado de la Auditoría	5
a. Análisis de Vulnerabilidades y pruebas de negación de servicio.	5
b. Pruebas de Caja Negra.....	6
c. Validación del Sistema Informático y de sus bases de datos.	7
IV. Conclusiones	7

I. Resumen General

El 1° de Julio de 2018, en el Estado de Oaxaca se llevará a cabo el desarrollo del proceso local electoral, en el que se elegirán Diputados Locales y Presidentes Municipales, por lo que el Instituto Estatal Electoral y de Participación Ciudadana (IEEPCO), contrato a la empresa PoderNet, para la implementación y operación del Sistema Informático del Programa de Resultados Electorales Preliminares, en donde se realizarán las fases del proceso operativo de acopio, digitalización, captura y verificación de datos, así como la publicación de resultados de las Actas PREP¹.

Por otra parte, el IEEPCO realizó la contratación de la empresa Marketin e Investigación S.A de C.V para la prestación del servicio de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Electorales Preliminares (PREP), para el Proceso Electoral Local Ordinario 2017-2018, con la finalidad de evaluar su integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados electorales.

Por lo que en cumplimiento a lo que establece el capítulo III, numeral 5, 7, 8 y 10 del Anexo 13 “Lineamientos del Programa de Resultados Preliminares (PREP) y Art. 347 numeral 1 inciso a) del Reglamento de Elecciones, para el Proceso Electoral Ordinario Dos Mil Dieciocho en el Estado de Oaxaca, Marketin e Investigación, realizó una auditoría de verificación y análisis del sistema informático del PREP 2018 - OAXACA, a fin de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de resultados, realizando para ello pruebas funcionales de caja negra al sistema informático para evaluar el procesamiento de la información y la generación de resultados preliminares, así como un análisis de vulnerabilidades, considerando al menos pruebas de penetración y revisión de configuraciones a la infraestructura tecnológica del PREP, que permitan evaluar la integridad en el procesamiento de la información de las Actas PREP para la elección de Diputados Locales y Presidentes Municipales, para la generación de resultados preliminares.

Durante este proceso de auditoría, se realizaron pruebas para verificar que el sistema informático del PREP, permitiera la captura, digitalización y publicación de los datos asentados en las Actas de Escrutinio y Cómputo (AEC) de las casillas que se reciben en los 86 CATD’s, y que fueron autorizados por el IEEPCO.

Como resultado de la auditoría al sistema informático para el procesamiento de los resultados electorales preliminares de la jornada electoral del 1° de junio del 2018, para la elección de Diputados Locales y Presidente Municipales, se concluye que el sistema es funcional para llevar a cabo la digitalización, captura y publicación de los resultados preliminares de las AEC, procesando de manera íntegra la información, y coadyuvando en todo momento con la transparencia de la información, al momento de ser publicada vía internet; ya que este sistema informático proporciona la seguridad de información al contar con estructuras de seguridad robustas y flexibles que permiten dar funcionalidad, capacidad, continuidad y seguridad a la infraestructura del PREP.

¹ Acta PREP. Primera copia del acta de escrutinio y cómputo destinada para el PREP, o en ausencia de ésta, cualquier copia del acta de escrutinio y cómputo.

II. Desarrollo de la Auditoría

A partir del mes de mayo, Marketing e Investigación, inició y llevó a cabo la realización de la auditoría de verificación y análisis al sistema informático del PREP y su infraestructura, atendiendo a cuatro líneas de trabajo como alcance de las pruebas a realizar:

1. Pruebas Funcionales de Caja Negra, con el que se evalúa la integridad en el procesamiento de la información y la generación de resultados preliminares para su publicación, analizando el funcionamiento y procesos de la aplicación en las fases de digitalización, captura y publicación de resultados, verificando que los datos capturados en las Actas PREP tengan correspondencia con los presentados en la publicación de resultados, mediante las formas de presentación de los mismos, considerando datos, imágenes y bases de datos.
2. Pruebas de vulnerabilidades en la infraestructura tecnológica del PREP (pentest y revisión de configuraciones de seguridad).
3. Pruebas de negación de servicio, pruebas de inyección de código malicioso y pruebas de acceso a los diversos recursos del sistema informático; así como pruebas al Sitio principal del IEEPCO.
4. Validación del sistema informático del PREP y de sus bases de datos;

Siendo revisado el sistema informático a partir del análisis a las aplicaciones que utiliza el sistema en el proceso de digitalización en los CATD remotos, su verificación, captura y publicación de los datos asentados en las Actas PREP, para la elección de Diputados Locales y Presidentes Municipales, con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados, conforme a lo considerado en el Proceso Técnico Operativo del PREP para el Proceso Electoral Ordinario Local 2017-2018 en el Estado de Oaxaca y en el Anexo 13 Lineamientos del Programa de Resultados Electorales Preliminares (PREP):

- En el que a través de los 86 CATD remotos instalados en los Consejos Distritales y Consejos Municipales, se realiza el acopio, digitalización y transmisión de la imagen de las Actas de Escrutinio y Cómputo (AEC) al CCV².
- Validación y Captura, la cual se realiza en el CCV con la información de la imagen digitalizada del Acta PREP, llevando a cabo la validación y captura correspondiente de los resultados de la votación, almacenando de manera correcta en la base de datos del sistema, tanto las imágenes codificadas para seguridad de la información, como los datos numéricos plasmados en dichas actas.
- Consulta y Publicación de resultados, en donde el sistema de manera interna, realiza los procesos de validación, restricciones, suma de votos, cálculo de porcentajes de participación, entre otros, proporcionando datos validos en las diferentes operaciones en las cuales se espera un resultado de votación y porcentaje, y en el que a través de una dirección electrónica de internet, se pone a disposición de la población en general, los resultados de la votación obtenida por partido o coalición de la elección a Diputados Locales y Presidentes Municipales, con un nivel de consulta

² CCV. Centro de Captura y Verificación

general, por distrito y por municipio, pudiendo consultar los resultados preliminares hasta nivel casilla, con la imagen del AEC, teniendo el sistema a este nivel, debido a la prueba piloto del PREP-casilla en 100 CAES³ con un máximo de 250 casillas para el día 1° de julio de 2018, la identificación de la forma de acopio y transmisión del Acta PREP al CCV.

Por lo que con base en el desarrollo de las acciones realizadas y con apego a los lineamientos del Programa de Resultados Electorales Preliminares, se desprenden a continuación los siguientes resultados.

III. Resultado de la Auditoría

a. Análisis de Vulnerabilidades y pruebas de negación de servicio.

Con fecha 20 de junio de 2018, se realizó al sistema informático pruebas de penetración (pentes), desde el exterior de la red de datos del PREP, contemplando servidores, aplicaciones web, equipo de telecomunicaciones y estaciones de trabajo; y la revisión de las configuraciones de los dispositivos que conforman la infraestructura tecnológica, así como la realización de ataques de negación de servicio con la finalidad de generar tráfico de red, hacia los servicios web que se publican dentro del dominio de la dirección electrónica donde se visualizarán los resultados electorales preliminares considerando: tráfico de red NO malintencionado, tráfico de red malintencionado de manera concurrente, con ataques volumétricos por protocolo TCP, UDP, ICMP de al menos 400 Mbps de throughput, realizando al menos Syn Flood, DNS Amplification, ICMP Flood respectivamente, y enviando ataque en la capa de aplicación (HTTP).

En el que se analizaron los parámetros de configuración y se identificaron fortalezas y área de oportunidad con la aplicación de buenas prácticas de seguridad en materia informática; así mismo, pruebas de escaneo de puertos, detección de vulnerabilidades y denegación de servicio (DOS) al sitio web proporcionado para la simulación de ataques; pruebas de seguridad y conexión de los servidores, y del cual, se emitió con fecha 20 de junio, el informe preliminar 001 “Pruebas de Vulnerabilidades a la Infraestructura Tecnológica y Pruebas de negación de servicio al sitio WEB de Publicación de Resultados del PREP”, en el que se concluye que como resultado del análisis de vulnerabilidad a las medidas y servicios adoptados para el sistema informático del PREP, proporcionan la seguridad de información al contar con estructuras de seguridad robustas.

Por lo que una vez que se dio conocimiento al Instituto Estatal Electoral y de Participación Ciudadana de Oaxaca, se concluye que derivado de los hallazgos encontrados en las pruebas realizadas, se determinó que el Sistema Informático del PREP, cumple con los lineamientos y no representa riesgo en su operatividad, funcionalidad, capacidad, continuidad y seguridad para la publicación de los resultados, mostrando que el sistema fue capaz de mitigar todas las vulnerabilidades a las que fue sometida, haciéndolo un sistema seguro.

³ CAES. Capacitador- Asistente Electoral Local

De igual forma con fecha 25 de junio, se realizaron las pruebas de vulnerabilidades en la infraestructura tecnológica del PREP (pentest y revisión de configuraciones de seguridad), así como pruebas de negación de servicio, pruebas de inyección de código malicioso y pruebas de acceso a los diversos recursos del sistema informático del sitio principal del IEEPCO; realizando ataques de negación de servicio con la finalidad de generar tráfico de red, hacia el dominio de la dirección electrónica “www.ieepco.org.mx”: tráfico de red NO malintencionado, tráfico de red malintencionado de manera concurrente, y del cual, se emitió con fecha 26 de junio, el informe preliminar 002 “Pruebas de Vulnerabilidad y de negación de servicio al sitio del Instituto Estatal Electoral y de Participación Ciudadana de Oaxaca (IEEPCO)”, en el que se emitieron las recomendaciones y soluciones pertinentes para reforzar las medidas de configuración y servicio, como parte difusora de la información del proceso electoral del 1° de julio de 2018.

b. Pruebas de Caja Negra.

Con base en el Proceso Técnico Operativo del PREP para el Proceso Electoral Ordinario Local 2017-2018 en el Estado de Oaxaca, se realizaron pruebas de caja negra al sistema informático del PREP, que permitió a Marketin, verificar y comprobar que en el sistema se puede capturar, procesar y desplegar diversos tipos de reporte de los resultados electorales preliminares, considerados también en el Anexo 13 de los lineamientos del PREP.

Por lo que con base en el numeral 7 del Proceso Técnico Operativo del PREP, se realizó la visita a los 86 CATD instalados en los Consejos Distritales y Municipales, a fin de verificar la infraestructura con que cuentan para llevar a cabo el proceso de acopio, digitalización y transmisión de las Actas PREP al CCV para su captura, validación y publicación de los resultados electorales, emitiendo para ello el informe parcial 001 “Resultados de la visita y verificación en campo realizada a los CATD remotos y al CCVE”, de fecha 28 de mayo, así como del informe final 002 del 11 de junio, en el que se da cuenta de los resultados obtenidos durante la verificación a la infraestructura, equipamiento y de comunicaciones instaladas por la empresa PoderNet, para dar respuesta al proceso técnico operativo.

Así también como parte de la auditoría con base en el numeral 16, Capítulo VI del Anexo 13 de los Lineamientos del PREP, se verificó la realización de los tres simulacros para la operación del sistema informático del PREP, como parte de las pruebas de caja negra para determinar su funcionalidad en el proceso de acopio, registro, digitalización, validación, captura, transmisión y recepción de las Actas PREP desde los 86 CATD previamente verificados, y que fueron instalados en los Consejos Distritales y Municipales, emitiendo para ello, dos informes del Desempeño de los Simulacros del PREP, del día 10 y 24 de junio, informando de las incidencias detectadas en la infraestructura y en el proceso de operación del sistema informático, a la conclusión de los mismos con la empresa encargada del PREP.

Con fecha 28 de junio de 2018, se concluyó con la realización de la prueba de caja negra a partir de información simulada y precargada en el sistema informático del PREP, verificándose que los

procesos de validación, restricciones, suma de votos, porcentajes de participación, despliegue de datos, entre otros, proporcionen datos validos en las diferentes operaciones en las que se obtendrán los resultados de votación y porcentajes, comprobando que los datos procesados coincidan con lo que se publica en pantalla para la elección de Diputados Locales y Presidentes Municipales, en sus diferentes formas de desagregar y presentar los resultados electorales preliminares para el día de la Jornada Electoral del 1° de Julio, realizando en ese mismo día, los comentarios pertinentes a la empresa encargada del PREP, ya que a partir de los criterios considerados por Marketin, tomando como base los lineamientos del Programa de Resultados Electorales Preliminares, se emitió el Informe Preliminar 003 “Resultados de las Pruebas Funcionales de Caja Negra”.

c. Validación del Sistema Informático y de sus bases de datos.

Durante el proceso de auditoría se estuvo realizando la verificación de las bases de datos en donde se efectúa el almacenamiento de la información de la Actas PREP, generando las huellas criptográficas en SHA-256 del software del PREP.

De igual forma, se verifico conforme al numeral 29, Capítulo II, Anexo 13 Lineamientos del PREP, que la base de datos con los resultados electorales preliminares contenidos en un formato de archivo CSV y de acuerdo a la estructura establecida por el Instituto, cumple con lo requerido.

El día de la jornada electoral, previo a la operación del PREP, se verificará el contenido de las bases de datos, a través de la ejecución de herramientas de administración de bases de datos que permitan determinar que no se encuentra ningún valor registrado en la base de datos como lo marca el numeral 14, Capítulo IV del Anexo 13 de los Lineamientos del PREP, y que las huellas criptográficas correspondan a lo previamente obtenido para llevar a cabo la validación del Sistema Informático del PREP.

IV. Conclusiones

- Durante los análisis realizados al sistema informático del PREP, se cumplieron con los criterios de valoración establecidos por Marketin, con apego al Proceso Técnico Operativo y del Anexo 13 de los Lineamientos del PREP para el Proceso Electoral Ordinario Local 2017-2018 en el Estado de Oaxaca.
- Que considerando la auditoría realizada para la inspección de los procesos del Sistema Informático del PREP, incluyendo las vulnerabilidad a los activos seleccionados, así como a la revisión de la configuración de los mismos, se tiene lo siguiente:
 - ✓ Las pruebas de caja negra mostraron que el programa es funcional para la elección de Diputados Locales y Presidentes Municipales.

- ✓ Se determinó que la forma de operar el sistema informático del PREP, para la publicación de resultados, cuenta con las medidas de seguridad para evitar que se modifiquen de manera injustificada la información de las Actas de Escrutinio y Cómputo.
- ✓ Las pruebas de análisis de vulnerabilidades mostraron que el sistema mitigó todas las vulnerabilidades a las que fue sometida, y que se subsanaron las observaciones emitidas tanto al Sistema Informático del PREP.
- Así mismo, Marketin e Investigación, durante el inicio de la operación de la publicación de resultados electorales preliminares de la jornada electoral del día 1° de julio, realizará verificaciones para validar que el programa auditado sea el que estará operando en ese día.

Atentamente

C. Santiago Morales Andrade
Representante Legal de la Empresa
Marketin e Investigación