INSTITUTO ESTATAL ELECTORAL
CHIHUAHUA

INFORME TÉCNICO

Auditoría a los sistemas PREP y PREP Casilla 2024

L.I. José Rómulo Bailón Barrón
M.I. Oscar Beltrán Gómez
M.I. Arión Ehécatl Juárez Menchaca
M.S.I. Sergio Antonio Talavera Carbajal

Índice

Introducción

El Programa de Resultados Electorales Preliminares (PREP) del Instituto Estatal Electoral de Chihuahua (IEE) se encarga de ofrecer resultados preliminares de las elecciones, utilizando para ello datos de las actas de escrutinio y cómputo recopiladas en las casillas electorales. Estos resultados tienen un carácter informativo y no definitivo, puesto que son publicados antes de la declaración oficial de los resultados electorales. La infraestructura del PREP y PREP Casilla se someten a auditorías regulares para garantizar la integridad, disponibilidad y seguridad en el manejo y procesamiento de la información electoral, de acuerdo con la normativa aplicable establecida por el Reglamento de Elecciones del INE y otros lineamientos relacionados.

La auditoría de la infraestructura del PREP y PREP Casilla es una medida esencial para asegurar la confiabilidad del sistema. Esta auditoría se lleva a cabo según lo estipulado por el Reglamento de Elecciones del INE, específicamente en la sección cuarta del capítulo II, título I, Libro Tercero, así como en el título II del Anexo 13 de los Lineamientos del PREP. El propósito de estas auditorías es verificar y analizar tanto la infraestructura física como los sistemas informáticos utilizados, para garantizar la integridad, disponibilidad y seguridad de los datos durante el proceso electoral. Estas evaluaciones son fundamentales para mantener la confianza en el proceso y asegurar que los resultados preliminares reflejen con precisión las votaciones registradas.

AUDITORÍA AL SISTEMA INFORMÁTICO Y A LA INFRAESTRUCTURA TECNOLÓGICA DEL PREP

I. Informe. Análisis de vulnerabilidades a la infraestructura tecnológica

El análisis de vulnerabilidades tiene como finalidad evaluar la seguridad de la infraestructura tecnológica del Organismo Público Local (OPL) del Instituto Estatal Electoral (IEE) de Chihuahua. Este proceso busca identificar y clasificar las vulnerabilidades para recomendar medidas correctivas y verificar su implementación efectiva.

Éste análisis abarca un examen exhaustivo que incluye desde la verificación de la red de comunicaciones y el sistema de cableado eléctrico, hasta la evaluación de riesgos de seguridad. Las principales etapas de este análisis son:

Identificación de Debilidades: Se realizan pruebas de penetración y se revisan los equipos y configuraciones de seguridad para detectar puntos débiles en la infraestructura tecnológica.

Clasificación y Documentación de Vulnerabilidades: Se catalogan las vulnerabilidades según su gravedad y se documentan detalladamente. Esta información se utiliza para elaborar recomendaciones dirigidas al OPL sobre las acciones correctivas necesarias.

Verificación de Medidas Implementadas: Se examina si las medidas de mitigación adoptadas por el OPL han sido efectivas en abordar las vulnerabilidades identificadas, asegurando así que se han resuelto de manera adecuada.

Este proceso es fundamental para fortalecer la seguridad de la infraestructura tecnológica y protegerla contra posibles amenazas.

En este sentido, se llevó a cabo un análisis de la infraestructura del Organismo Público Local (OPL), utilizando una combinación de entrevistas con el personal técnico y un cuestionario específico. Este enfoque permitió recoger información esencial sobre el estado actual de los sistemas y equipamiento. Seguido de esto, se realizó una inspección física de las áreas y elementos críticos de la infraestructura. Esta metodología facilita la identificación de áreas susceptibles de mejora, con el fin de prevenir riesgos y fallos que podrían comprometer la operatividad y seguridad.

La auditoría de seguridad realizada a la infraestructura tecnológica del Programa de Resultados Electorales Preliminares (PREP) y la red electoral está orientada a detectar y documentar cualquier vulnerabilidad existente. El propósito central de este procedimiento es desarrollar y proponer recomendaciones efectivas que permitan mitigar dichas vulnerabilidades de manera oportuna, garantizando así la integridad y resiliencia de los sistemas frente a amenazas potenciales. Este enfoque no solo refuerza la seguridad sino que también respalda la transparencia y confiabilidad del proceso electoral.

Para realizar la auditoría a la infraestructura del OPL se realiza la visita a las oficinas centrales y al centro operativo el 22 de mayo de 2024. En estas visitas se destaca lo siguiente:

IEE Oficinas Centrales

En términos generales, se concluye que la red de datos **CUMPLE SATISFACTORIAMENTE** con la evaluación realizada, basada en el cuestionario y la inspección visual efectuados durante esta auditoría.

IEE Asamblea Municipal de Chihuahua

Se considera que esta asamblea **CUMPLE SATISFACTORIAMENTE DE MANERA PARCIAL** con la auditoría realizada debido a que las instalaciones no están en condiciones óptimas, especialmente en lo referente al sistema de climatización y al cableado de red. Sin embargo, se entiende que estas instalaciones son temporales y fueron adaptadas específicamente para el proceso electoral del próximo 2 de junio de 2024. Teniendo esto en cuenta, se considera que las instalaciones cubrirán los requerimientos necesarios para el correcto desarrollo del proceso electoral. Sería recomendable disponer de un espacio dedicado exclusivamente al proceso de captura del PREP, que cumpla con las especificaciones necesarias para tal fin.

IEE CCV Chihuahua

Se considera importante realizar un análisis completo y una corrección oportuna para fortalecer la infraestructura. Esto garantizará la integridad y estabilidad del sistema, minimizando el riesgo de interrupciones o compromisos de seguridad durante el desarrollo del proceso electoral. Se considera que el CCV Chihuahua **CUMPLE DE MANERA PARCIAL** con la auditoría efectuada.

Análisis de vulnerabilidades a la red interna del IEE de Chihuahua

La red interna del Instituto Estatal Electoral (IEE) de Chihuahua, al igual que cualquier sistema de tecnología de la información, está expuesta a diversas vulnerabilidades que pueden comprometer su integridad y seguridad. Estas vulnerabilidades pueden ser aprovechadas por atacantes con el fin de obtener acceso no autorizado a la red. Una vez que los atacantes han logrado infiltrarse, tienen la capacidad de ejecutar una variedad de acciones malintencionadas. Estas acciones pueden incluir la sustracción de datos confidenciales, la alteración o destrucción de información crítica, y la interrupción de los servicios esenciales del IEE.

La explotación de estas vulnerabilidades no solo pone en riesgo la seguridad de los datos almacenados, sino que también puede tener consecuencias graves para la operación y reputación del Instituto. Los datos confidenciales, como información personal de los empleados, registros electorales y resultados de votaciones, pueden ser robados y utilizados de manera indebida. Además, la alteración de los datos puede afectar la precisión y confiabilidad de los procesos electorales, lo que podría generar desconfianza entre la ciudadanía y socavar la credibilidad del sistema electoral.

Por estas razones, es fundamental implementar medidas de seguridad robustas y realizar evaluaciones periódicas de vulnerabilidades para proteger la red interna del IEE. Estas

medidas deben incluir la actualización constante de los sistemas, la instalación de parches de seguridad, la formación de los empleados en prácticas seguras y la realización de auditorías de seguridad regulares. Solo a través de un enfoque proactivo y multifacético se puede garantizar la protección de la red contra posibles amenazas y asegurar la continuidad y fiabilidad de los servicios del Instituto Estatal Electoral de Chihuahua.

En la evaluación de la seguridad de la red interna del IEE de Chihuahua, se emplearon sistemas avanzados de análisis. A continuación, se resumen los principales hallazgos del análisis:

- Vulnerabilidades Informativas: La mayoría de las vulnerabilidades detectadas en el servidor web del PREP fueron clasificadas como de prioridad informativa. Esto indica que son de muy bajo riesgo e impacto, generalmente relacionadas con información que podría ser útil para entender mejor la configuración y seguridad del sistema, pero que no constituyen una amenaza inmediata.
- Media Prioridad: Solo fue encontrada una vulnerabilidad de prioridad Media, relacionada con el Certificado SSL del sitio web. Estas no representan riesgos potenciales significativos y suelen requerir acciones correctivas como actualizaciones o modificaciones en la configuración de las aplicaciones para mitigar los riesgos asociados.

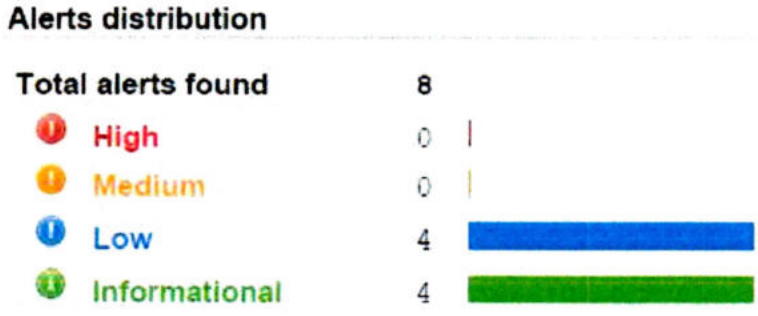

Imagen 1.1. Alertas detectadas.

Los resultados de la auditoría a las oficinas centrales del Instituto Estatal Electoral (IEE) de Chihuahua indican que en términos generales, la infraestructura cumple con los requisitos establecidos, aunque se destacan algunas áreas que requieren mejoras, especialmente en aspectos básicos.

Aunque las vulnerabilidades detectadas en el sistema no representan un riesgo alto para la seguridad y funcionamiento del sistema, es crucial abordar estos hallazgos lo antes posible para mantener la integridad operativa. Además, se enfatiza la importancia de contar con la presencia activa del personal técnico durante la jornada electoral para prevenir y resolver cualquier incidencia técnica que pueda surgir.

Este enfoque proactivo en la gestión técnica y la respuesta rápida a las vulnerabilidades son esenciales para asegurar la eficiencia y seguridad de las operaciones electorales en el estado de Chihuahua.

II. Informe. Pruebas de denegación de servicios y pruebas de estrés al sistema PREP.

Introducción

Los ataques distribuidos de denegación de servicio (DDoS) constituyen un riesgo considerable para la infraestructura de red de las empresas. Estos ataques intentan saturar los sistemas con un exceso de tráfico, bloqueando el acceso a sitios web y servicios corporativos. Los atacantes emplean diversos métodos para crear un volumen masivo de solicitudes, paquetes y datos fraudulentos, con el fin de sobrecargar los sistemas y causar interrupciones.

Aunque generalmente se asocian con actores maliciosos, los ataques DDoS también pueden ocurrir en contextos legítimos, como las pruebas de seguridad y rendimiento. Estas pruebas, llamadas "pruebas de estrés", son cruciales para evaluar la fortaleza de los sistemas ante altas demandas y asegurar su buen funcionamiento bajo presión. En eventos significativos,

como la publicación de resultados electorales, es común que los sitios web enfrenten un incremento considerable en el tráfico, lo que puede generar condiciones similares a un ataque DDoS debido a una demanda legítima de usuarios.

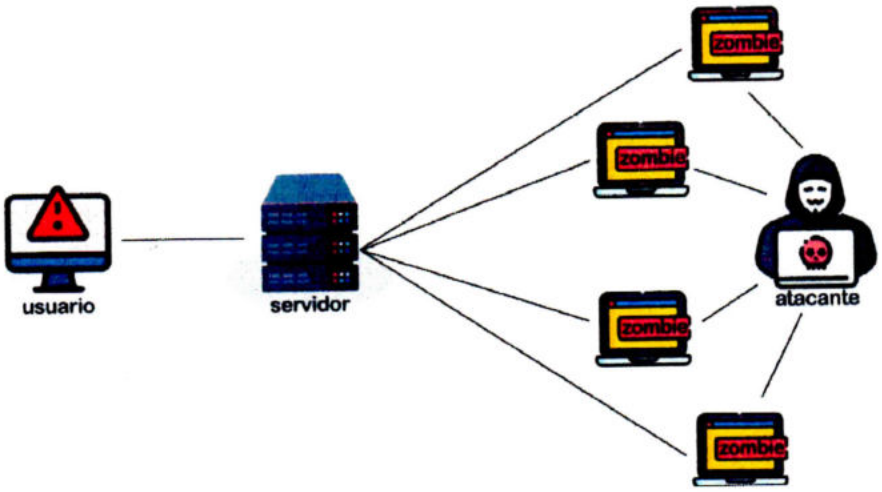

Imagen 2.1. Boceto de un ataque DDoS.

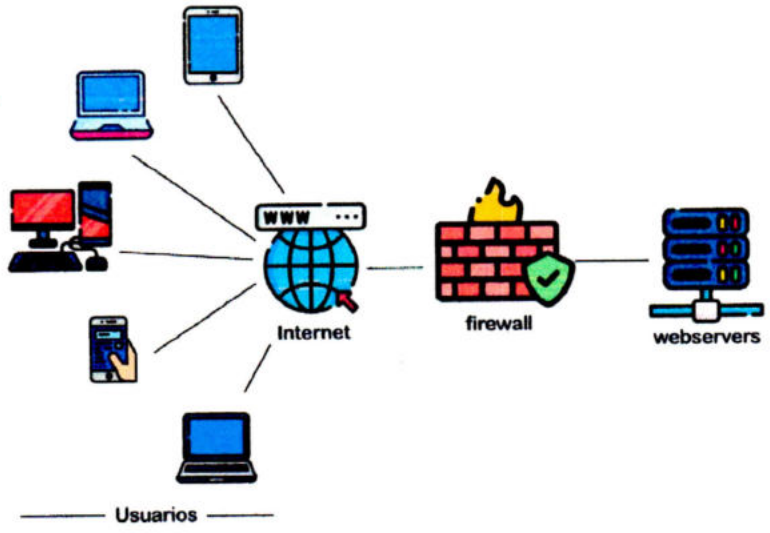

Imagen 2.2. Boceto de un ataque de Estrés.

Las pruebas de denegación de servicio (DoS) y las pruebas de estrés son técnicas utilizadas para medir la resistencia y capacidad de respuesta de los servicios web ante grandes volúmenes de tráfico. Estas pruebas emulan un ataque de denegación de servicio distribuido (DDoS) o una alta carga de usuarios legítimos, respectivamente, para evaluar el desempeño de la infraestructura bajo presión. (Imagen 2.1 y 2.2)

El objetivo principal de estas pruebas es identificar posibles vulnerabilidades en la infraestructura de red y en los sistemas de aplicaciones que podrían fallar o deteriorarse significativamente bajo condiciones de estrés. Se envían múltiples solicitudes simultáneas a los servicios web para observar cómo manejan los picos de tráfico, tanto en la infraestructura del Organismo Público Local (OPL) como en la infraestructura proporcionada por terceros.

Este tipo de pruebas es fundamental para:

1. Garantizar la disponibilidad: Asegura que el sitio web o servicio permanezca operativo incluso en condiciones extremas.
2. Optimizar el rendimiento: Permite a los administradores ajustar y mejorar las configuraciones para manejar volúmenes de tráfico inesperadamente altos.
3. Preparación para escenarios de crisis: Ayuda a prepararte para ataques reales, permitiendo a los equipos de TI desarrollar planes de respuesta más efectivos.

Las pruebas de denegación de servicio se dividen en tres categorías:

- **Tráfico normal y no malintencionado:** Simula el tráfico legítimo esperado en un día de alta actividad mediante transacciones sintéticas.
- **Tráfico saturado y no malintencionado:** Simula el tráfico legítimo pero en condiciones de saturación debido a un interés inusual.
- **Tráfico de red malintencionado:** Consiste en paquetes de red malformados, incluyendo:
    - Ataques volumétricos por protocolo TCP
    - Ataques volumétricos por protocolo UDP

- Ataques volumétricos por protocolo ICMP
- Ataques en la capa de aplicación (HTTP y HTTPS)

El Instituto Estatal Electoral (IEE) de Chihuahua, como parte del desarrollo de su infraestructura y equipo para la publicación de los resultados preliminares de las próximas elecciones, ha contratado los servicios de AWS para el despliegue y publicación de dichos resultados. AWS es una plataforma que ya incluye servicios para bloquear direcciones sospechosas de ataques DDoS.

Las configuraciones de seguridad de AWS demostraron ser altamente efectiva en las tres categorías antes mencionadas en la mitigación de los ataques DDoS simulados. La infraestructura del IEE de Chihuahua, alojada en AWS, mantuvo su operatividad y rendimiento durante las pruebas, sin sufrir interrupciones significativas. Estos resultados confirman que la plataforma PREP está preparada para manejar situaciones de alta demanda y soportar posibles ataques, asegurando la disponibilidad y seguridad de los servicios durante eventos críticos como la publicación de resultados electorales.

Sin embargo, es importante señalar que toda tecnología puede ser vulnerada debido a los constantes cambios tecnológicos. Por esta razón, es crucial mantener actualizadas las configuraciones de seguridad y adaptarse rápidamente a las nuevas amenazas y desafíos que puedan surgir en el entorno digital.

Informe Prototipo Navegable

Se ha realizado un análisis de la conformidad del sitio Programa de Resultados Electorales Preliminares 2024 (PREP) utilizando sus herramientas de validación en línea en conjunto con algunas herramientas alternativas para complementar el análisis.

Nos complace informar que, en general, los resultados obtenidos son positivos y confirman la conformidad del sitio con los estándares web.

Durante el proceso de validación, se identificaron algunos errores menores y advertencias que, aunque no afectan significativamente el comportamiento del sitio, merecen atención y consideración para mantener la calidad y la consistencia del código.

Informe de Seguridad de PREP Casilla

Las pruebas se realizaron conforme a los lineamientos de seguridad establecidos y se enfocan en garantizar que la API es segura y cumple con las mejores prácticas de la industria. El objetivo de este informe es proporcionar una evaluación de las medidas de seguridad implementadas en las API Rest y confirmar que dichas medidas cumplen con los estándares de seguridad pertinentes.

Las pruebas de seguridad realizadas incluyeron, pero no se limitaron a, los siguientes aspectos:

1. Autenticación y Autorización
2. Control de Acceso
3. Cifrado de Datos
4. Pruebas de Vulnerabilidad

Después de realizar pruebas de seguridad, se concluye que las API Rest del PREP Casilla cumplen con los lineamientos de seguridad pertinentes y están adecuadamente protegidas contra posibles amenazas. Las medidas de seguridad implementadas, incluyendo la autenticación JWT y el hosting en AWS, son efectivas y garantizan la integridad y confidencialidad de los datos.

Simulacros.

A lo largo de los tres simulacros y de las pruebas a las que fue sometido el sitio de publicación del Prep 2024 se ha observado que:

- Son perceptibles las mejoras y el nivel de infraestructura del sitio, de acuerdo a los tres simulacros realizados.
- Los ajustes realizados a los largo de las tres jornadas de simulacro dan un buen precedente del nivel técnico y del tiempo de respuesta por alguna contingencia.
- Las pruebas arrojaron resultados **satisfactorios** en los niveles de carga y estrés.

Los ajustes, pruebas y la configuración de los simulacros generan un buen grado de certeza en el comportamiento del sitio de las publicaciones PREP en las futuras elecciones del 2 de junio, sin embargo, y particularmente por la naturaleza tecnológica de los sitios Web, no es posible asegurar en un 100% que el sitio de publicación PREP así como cualquier otro sitio presente en Internet, se encuentre libre de ataques y posibles vulnerabilidades.

III. Validación del sistema informático del PREP y de sus bases de datos, ante un tercero con fé pública

La validación del sistema informático del Programa de Resultados Electorales Preliminares (PREP) y de sus bases de datos ante un tercero con fe pública es un proceso formal y transparente mediante el cual se verifica la integridad, la seguridad y el correcto funcionamiento del sistema utilizado para el conteo y la difusión de los resultados preliminares de una elección.

En este proceso, un tercero con fe pública, que puede ser una entidad independiente, un organismo gubernamental o un profesional debidamente autorizado, realiza una evaluación exhaustiva del sistema informático del PREP y de todas las bases de datos asociadas. Esta

validación se lleva a cabo siguiendo procedimientos y estándares rigurosos, con el objetivo de garantizar la imparcialidad y la objetividad del proceso.

Durante la validación, se verifica que el sistema informático del PREP esté configurado correctamente y que cumpla con todos los requisitos técnicos y legales establecidos para asegurar la transparencia y la confiabilidad del proceso electoral. También se realiza una revisión detallada de las bases de datos para confirmar que estén completas, precisas y libres de cualquier tipo de manipulación o alteración indebida.

La presencia de un tercero con fe pública en este proceso brinda una garantía adicional de que la validación se realiza de manera imparcial y objetiva, y que los resultados obtenidos son fiables y verificables. Esto contribuye a fortalecer la confianza pública en el sistema electoral y en la integridad de los resultados preliminares de la elección.

En este informe se presentan los resultados de la auditoría realizada al sistema PREP y a sus bases de datos, así como los hallazgos identificados. Estos hallazgos servirán como base para abordar de manera oportuna cualquier problema relacionado con los sistemas y procedimientos que se utilizarán antes, durante y después de las elecciones.

Validación y verificación de los sistemas informáticos PREP y PREP Casilla

Para la validación y verificación de los sistemas que serán utilizados el día de la jornada electoral, se llevaron a cabo los siguientes análisis:

Base de datos. El análisis se centra en la inspección detallada de las tablas para verificar que no existan votos capturados antes del conteo oficial. Para ello, se realiza una revisión y se imprime el estatus de las tablas que almacenan la información.

Pruebas de caja negra.

Las pruebas de caja negra en un sistema informático son un método de testing en el que los evaluadores examinan la funcionalidad del sistema sin conocer su estructura interna o el código fuente. Se enfocan en verificar si el sistema cumple con los requisitos especificados y produce las salidas correctas para una serie de entradas dadas. El objetivo es detectar

errores o fallos en la funcionalidad del sistema desde la perspectiva del usuario final, asegurando que el sistema opere de acuerdo con sus especificaciones.

Conclusiones

Los sistemas PREP y PREP Casilla se observan aptos para su funcionamiento durante la jornada electoral del 2 de junio de 2024. En general, estos sistemas son confiables y entregan los resultados esperados basados en las entradas recibidas. Sin embargo, los informes parciales han revelado algunas oportunidades de mejora para hacer los sistemas más eficientes y robustos.

IV. Informe. Pruebas funcionales de caja negra al sistema informático del PREP

Se presenta un informe sobre la auditoría y análisis del sistema informático del Programa de Resultados Estadísticos Preliminares (PREP) del Instituto Estatal Electoral (IEE) de Chihuahua, a ser utilizado durante la jornada electoral del 2 de junio de 2024. La evaluación se enfoca en la integridad, disponibilidad y seguridad del sistema, abarcando pruebas funcionales de caja negra y análisis del proceso operativo completo. El objetivo principal es garantizar la confiabilidad y transparencia en el procesamiento de la información y la generación de resultados, en estricto apego a la normativa vigente.

El PREP juega un papel crucial en las elecciones, proporcionando resultados preliminares de manera oportuna y confiable. En este contexto, la auditoría y análisis del sistema informático son fundamentales para garantizar la integridad, disponibilidad y seguridad de la información procesada. El presente informe detalla los hallazgos y recomendaciones derivados de la evaluación realizada, con el objetivo de fortalecer el sistema y asegurar un proceso electoral transparente y confiable.

La auditoría se llevó a cabo mediante la realización de pruebas funcionales de caja negra, abarcando la totalidad del sistema PREP, incluyendo:

- **Recepción de actas:** Se evaluó la capacidad del sistema para recibir actas de manera eficiente y segura, verificando la integridad y autenticidad de las mismas.
- **Escaneo de actas:** Se analizó la precisión y rapidez del proceso de escaneo, garantizando la correcta captura de los datos contenidos en las actas.
- **Captura de resultados:** Se evaluó la exactitud y confiabilidad de la captura de resultados, asegurando la correspondencia con los datos escaneados.
- **Publicación de resultados:** Se verificó la integridad y transparencia de la publicación de resultados, garantizando el acceso oportuno y confiable a la información para la ciudadanía.

Las pruebas de caja negra, también conocidas como pruebas funcionales o pruebas de comportamiento, son una técnica fundamental para evaluar la calidad del software. A diferencia de las pruebas de caja blanca, que se enfocan en el código fuente y la estructura interna del programa, las pruebas de caja negra se basan únicamente en las entradas y salidas del sistema para verificar su correcto funcionamiento.

Las observaciones del funcionamiento en general del Programa de Resultados Estadísticos Preliminares (PREP) y del PREP Casilla del Instituto Estatal Electoral (IEE) de Chihuahua tiene la finalidad de que se evalúe la prioridad de los mismos y puedan ser subsanados antes del día de las elecciones.

Conclusiones

La evaluación de caja negra realizada a los sistemas PREP y PREP Casilla del Instituto Estatal Electoral de Chihuahua, el 30 de mayo del 2024, fue satisfactoria. Los votos de las actas capturadas se procesaron adecuadamente según sus características, obteniendo los resultados esperados y publicándose correctamente.

V. Revisión de las pantallas del sitio de publicación del PREP, verificando el apego a las plantillas base de la interfaz proporcionadas por el INE

A simple vista, el sitio PREP en su versión de escritorio y móvil cumple con las plantillas base proporcionadas por el INE. Sin embargo, es difícil realizar una comparación detallada del código al no contar con los archivos CSS correspondientes y una estructura base HTML, es decir, un sitio de prueba para comparar el funcionamiento de ambos.

Podemos verificar esto comparando las pantallas propuestas por el INE con las pantallas vistas en el sitio PREP.

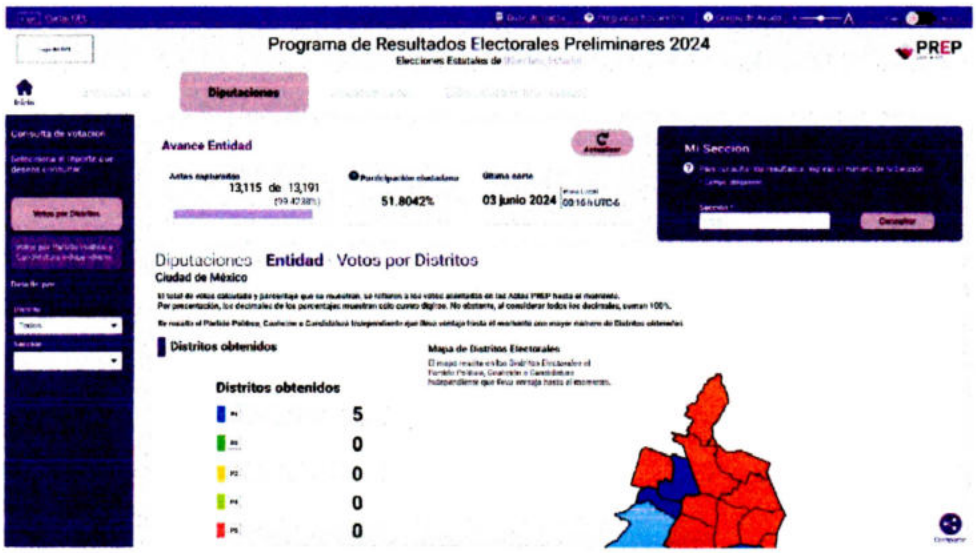

Imagen 5.1. Plantilla principal, propuesta por el INE.

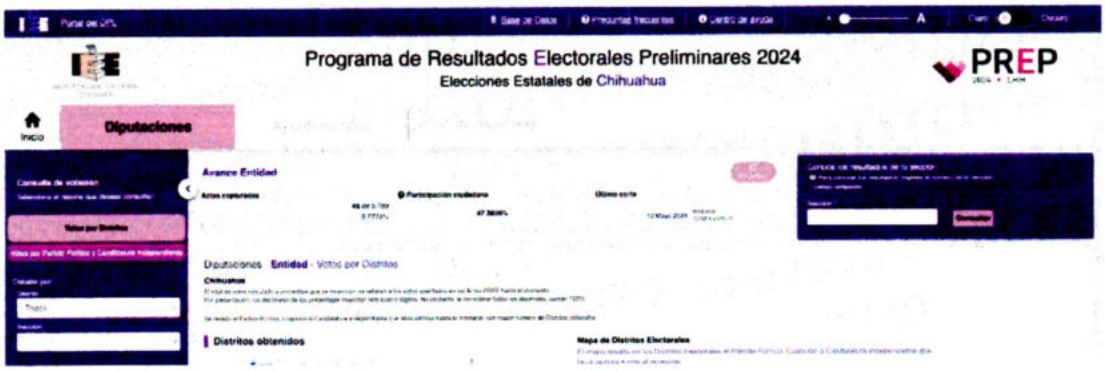

Imagen 5.2. Plantilla principal, desarrollada para el sitio PREP.

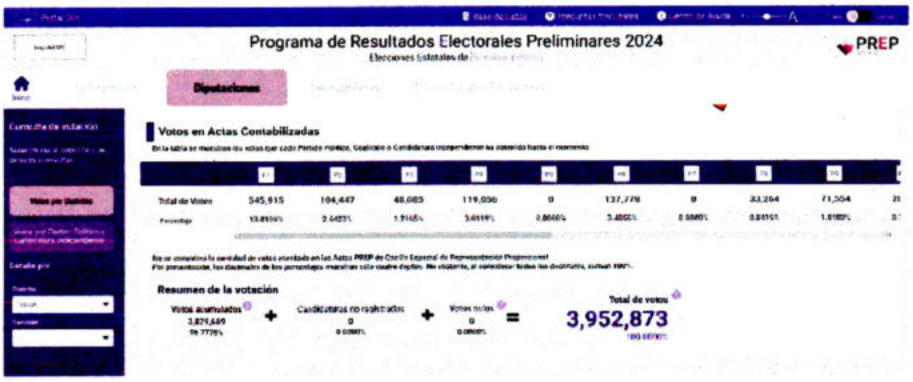

Imagen 5.3. Plantilla principal (resumen de votación), propuesta por el INE.

Imagen 5.4. Plantilla principal (resumen de votación), desarrollada para el sitio PREP.

Los resultados de la Auditoría muestran que la infraestructura, el sistema PREP y PREP Casilla son considerados aptos para su funcionamiento en el proceso electoral del 2 de junio de 2024. Los detalles y reservas de esta auditoría son entregados al IEE de Chihuahua en los informes técnicos correspondientes.

Ente Auditor

L.I. José Rómulo Bailón Barrón

M.I. Oscar Beltrán Gómez

M.I. Arión Ehécatl Juárez Menchaca

M.S.I. Sergio Antonio Talavera Carbajal