



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**

**Unidad Iztapalapa**

## **Auditoría del Programa de Resultados Electorales Preliminares para el Proceso Electoral Local Ordinario 2023-2024 en el estado de Oaxaca**

### **Informe Final**

---

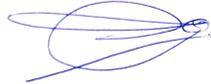
**29 de mayo de 2024**



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
Unidad Iztapalapa

## *Aprobación del Documento*

<b>Línea de Trabajo</b>	<b>Responsable</b>	<b>Firma</b>
Coordinador General del Convenio	Mtro. Omar Lucio Cabrera Jiménez	

29 de mayo de 2024



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
Unidad Iztapalapa

## *Historia de Cambios*

<b>Fecha</b>	<b>Versión</b>	<b>Autor</b>	<b>Descripción</b>
29/05/2024	0.1	OLCJ, LFCC	Versión inicial
29/05/2024	1.0	OLCJ y LFCC	Versión final



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
Unidad Iztapalapa

## Contenido

APROBACIÓN DEL DOCUMENTO.....	II
HISTORIA DE CAMBIOS.....	III
1. RESUMEN EJECUTIVO .....	1
2. INTRODUCCIÓN.....	3
3. RESULTADOS.....	3
3.1 RESULTADOS DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA .....	3
3.2 RESULTADOS DE LA VALIDACIÓN DEL SISTEMA INFORMÁTICO Y DE SUS BASES DE DATOS .....	4
3.3 RESULTADOS DEL ANÁLISIS DE VULNERABILIDADES A LA INFRAESTRUCTURA Y SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DONDE SE IMPLEMENTE EL PREP .....	6
3.4 PRUEBAS DE NEGACIÓN DE SERVICIO AL SITIO DE PUBLICACIÓN DEL PREP Y AL SITIO PRINCIPAL DEL IEEPCO.	6

## **1. Resumen ejecutivo**

El 26 de febrero de 2024, la UAM-I y el IEEPCO firmaron un convenio de colaboración para realizar la Auditoría al programa de resultados electorales preliminares, con motivo del Proceso Electoral Local Ordinario 2023-2024 en el Estado de Oaxaca teniendo como objetivo final validar ante la sociedad que el sistema informático del PREP es confiable y seguro.

La auditoría se realizó a través de 4 líneas de trabajo.

### **Pruebas funcionales de caja negra al sistema informático del PREP (PFCN)**

Las PFCN consisten en usar de una manera estructurada las funciones del sistema informático y validar que su comportamiento es como se espera de acuerdo con sus especificaciones, sin tomar en cuenta la forma en que está construido.

Se realizaron 2 ciclos de prueba aplicándose pruebas manuales para asegurar que el sistema funciona como se espera. Los hallazgos encontrados por el equipo de la UAM-I fueron notificados al equipo del IEEPCO, el cual los atendió y el equipo de la UAM-I verificó su correcta resolución.

De los resultados de las PFCN puede afirmarse que el sistema informático del funciona como se espera y no tiene funciones que no estén dentro de sus especificaciones.

### **Validación del sistema informático y de sus bases de datos ante un tercero con fe pública**

Esta validación tiene como objetivo asegurar que el sistema informático usado para el PREP 2024 es el mismo que fue auditado, así como asegurar que al iniciar la operación del PREP 2024, este inicializado correctamente y no existan actas con votación precargadas.

Para hacer la validación se elaboraron procedimientos para extraer las firmas electrónicas de los componentes y hacer consultas a las bases de datos del PREP 2024 lo cual permite hacer las validaciones previo al inicio, durante y al cierre de operaciones del PREP 2024.

Estos procedimientos serán utilizados los días de 2 y 3 de junio para las actividades de validación.



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
Unidad Iztapalapa

## **Análisis de vulnerabilidades a la infraestructura y servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP**

Esta línea de trabajo tiene como objetivo asegurar que el sistema informático del PREP 2024 está construido de manera segura y es resistente a ataques.

Se realizaron análisis de vulnerabilidades con pruebas de penetración (pentest) y revisión de configuraciones de la infraestructura y servicios relacionados con Tecnologías de Información y Comunicaciones donde se implementó el PREP; se hicieron pruebas de penetración, tanto en infraestructura basada en la *nube* como en la evaluación de un CATD.

Los hallazgos encontrados por el equipo de la UAM-I fueron notificados al equipo del IEEPCO, el cual los atendió y el equipo de la UAM-I verificó su correcta resolución.

De los resultados de esta línea de trabajo se puede afirmar que el sistema informático del PREP 2024 es seguro y es capaz de resistir ataques informáticos.

## **Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IEEPCO**

Esta línea de trabajo tiene como objetivo realizar ataques que envían gran volumen de peticiones a los servidores para intentar saturarlos para que sea posible identificar, evaluar y aplicar las medidas necesarias para asegurar la correcta y continua disponibilidad del servicio Web, así como de los sitios de publicación de resultados del PREP y del sitio principal del IEEPCO, durante el periodo de operación del PREP.

Se realizaron las pruebas de acuerdo con las especificaciones indicadas en el Anexo Técnico del Convenio de Colaboración y se comprobó que los mecanismos de protección del PREP 2024 funcionan de manera adecuada.

De los resultados de estas pruebas se puede afirmar que el sistema informático del PREP 2024 es capaz de resistir ataques de saturación.

En la realización de Auditoría participaron activamente 6 Profesores especializados en Desarrollo de Sistemas de Información, Ingeniería de Software y análisis de datos, así como 3 especialistas en seguridad informática y 11 alumnos de trimestres avanzados de las licenciaturas en Computación e Ing. Electrónica.

## **2. Introducción**

La auditoría al programa de resultados electorales preliminares PREP de 2024 es una actividad para aumentar la confianza de la ciudadanía en el instrumento y en los resultados que publique.

La realización de la auditoría implicó gran esfuerzo de los equipos de la UAM-I y del IEEPCO con un número grande de participantes (cerca de 40 personas) y casi 3 meses calendario.

Este documento presenta el Informe Final de la Auditoría al sistema informático del PREP 2024.

El reporte consta de un Resumen ejecutivo describiendo en términos generales las actividades realizadas y los resultados obtenidos.

A continuación de esta introducción se presentan los resultados de cada línea de trabajo de la auditoría.

## **3. Resultados**

### **3.1 Resultados de las pruebas funcionales de caja negra**

La metodología utilizada se basó en la observación del flujo que debe seguir la información de acuerdo con las descripciones asentadas en los documentos de requerimientos y el proceso técnico operativo (PTO).

Se efectuó la ejecución del flujo de información del sistema siguiendo las trayectorias primarias o correctas (happy path) y dejando al final los caminos alternos que en este sistema están considerados en el tratamiento de incidencias.

Para realizar las pruebas, se siguió el flujo natural de la información considerando tanto escenarios correctos como escenarios incorrectos en la dirección del flujo. Las pruebas se dividieron en 4 líneas:

1. Se realizaron los procesos de Digitalización, Captura y Publicación con énfasis en:
  - La verificación de que los Cálculos publicados sean correctos y
  - La verificación de que la Base de Datos que se descargó de la página del PREP no contenía actas al inicio del proceso.

Estas pruebas se realizaron durante los días 23, 24, 26 y 29 de abril del 2024.

2. Se realizaron los procesos de Digitalización, Captura y Publicación con énfasis en:



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
Unidad Iztapalapa

- La validación de los campos en tipo de dato y longitud del dato.

Esta prueba se realizó el día 26 de abril del 2024.

3. Se verificó el apego de la consulta del PREP a las plantillas proporcionadas por el INE y a las Normas Aplicables en:
  - Pantalla completa en aplicación de escritorio y
  - Aplicación móvil.

Estas pruebas se realizaron el día 30 de abril del 2024.

4. Se realizaron los procesos de Digitalización, Captura y Presentación con énfasis en:
  - Manejo de actas con incidencias y

Estas pruebas se realizaron el día 29 de abril del 2024.

En estas líneas se detectaron incidencias que fueron comunicadas al IEEPCO y al proveedor del Sistema PREP para su atención.

Las incidencias detectadas fueron de severidad baja y en ningún momento ponen en riesgo los resultados que genere el sistema del PREP.

En distintas reuniones con personal del proveedor y del IEEPCO se realizó la revisión de los hallazgos haciendo las aclaraciones correspondientes y registrando que las observaciones fueron atendidas.

En las Pruebas de apego a las plantillas base de la interfaz proporcionadas por el INE (descritas en la sección 3.3 del anexo técnico) para el sistema los hallazgos fueron reportados al IEEPCO y al proveedor. Por su severidad evaluada como Muy baja, no representan un riesgo para la operación del sistema PREP.

Por todo lo anterior se considera que el Sistema PREP 2024 cumple con los requerimientos funcionales y los resultados que genere serán el reflejo fiel de las actas que se registren.

### **3.2 Resultados de la Validación del Sistema Informático y de sus bases de datos**

Esta línea de trabajo plantea asegurar que el sistema informático del PREP en operación el 2 y 3 de junio sea el mismo que fue auditado y por lo mismo todas las conclusiones de la auditoría le son aplicables. Adicionalmente plantea una validación que no existan actas precargadas antes de que el sistema informático inicie sus operaciones.



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**

**Unidad Iztapalapa**

Las validaciones tienen que hacerse previo a la operación del PREP, durante la operación del PREP y al cierre de operaciones del PREP, estas validaciones deben hacerse ante un notario público.

Para validar que el sistema informático en operación es el mismo que el que fue auditado, se compara los elementos del sistema informático contra los del sistema auditado. La comparación de elementos se hace mediante la obtención de la firma criptográfica de cada elemento, la cual es única. Si dos elementos son iguales, sus firmas criptográficas son idénticas, si hay una variación por pequeña que sea, las firmas son diferentes.

Las firmas se obtienen mediante un algoritmo que procesa cada byte de un archivo y genera como resultado la firma criptográfica.

Para poder hacer la validación es necesario desarrollar procedimientos que tomen los archivos de los componentes del sistema informático, generen sus firmas criptográficas, hagan lo mismo con el sistema auditado y comparen las firmas.

Para validar que no hay actas precargadas, es necesario incorporar consultas a las bases de datos en los procedimientos ya mencionados.

Para poder realizar la validación se elaboró un Procedimiento de Validación que indica la forma en que se harán las distintas actividades de la VSIBD. Este procedimiento fue probado en los simulacros del PREP llevados a cabo los días 12, 19 y 26 de mayo, lo cual permitió hacer ajustes para una mejor ejecución durante el proceso de validación.

El Proceso de Validación se llevará a cabo los días 2 y 3 de junio utilizando procedimiento de Validación.

El resultado de la validación se dará a través de las Constancias de Hechos para los siguientes puntos del Proceso de Validación:

- Generación de las huellas criptográficas de los componentes, programas, configuraciones y, en su caso, códigos auditados del sistema informático del PREP.
- La validación de los componentes, programas, configuraciones y, en su caso, códigos auditados; y de las bases de datos del sistema informático del PREP.



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**

Unidad Iztapalapa

### ***3.3 Resultados del Análisis de vulnerabilidades a la infraestructura y servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP***

El objetivo de esta línea de trabajo es asegurar que el sistema informático del PREP 2024 está construido de manera segura y es resistente a ataques.

Se aplicaron herramientas automáticas de reconocimiento de vulnerabilidades y se analizaron los datos correspondientes. De este análisis se hicieron hallazgos que fueron reportados al equipo del IEEPCO, los cuales fueron resueltos. Posteriormente se rehicieron algunos análisis para asegurar que los hallazgos se hubieran resuelto. Todos los hallazgos tuvieron un nivel bajo de gravedad y no ponen en riesgo al sistema informático.

Esta línea de trabajo a su vez constituida por 2 sublíneas:

#### **1. Pruebas de penetración**

Consiste en la aplicación de pruebas intentando pasar las defensas del sistema informático.

Se realizaron estas pruebas de las cuales se hicieron hallazgos de bajo nivel de gravedad, los cuales fueron notificados al equipo del IEEPCO para su tratamiento. Posteriormente el equipo de la UAM-I validó su solución. Todos los hallazgos encontrados fueron resueltos y ninguno puso en riesgo la seguridad del sistema informático.

#### **2. Revisión de configuraciones**

Revisión a las configuraciones de todos los elementos del sistema informático del PREP y de su infraestructura tecnológica para asegurar que son las adecuadas en términos de seguridad de acuerdo con las mejores prácticas en esta materia.

Se revisaron las configuraciones de cada componente del sistema informático contra las recomendaciones de las mejores prácticas. De esta revisión se hicieron hallazgos que fueron atendidos por el equipo del IEEPCO y validada su solución por el equipo de la UAM-I. Los hallazgos fueron de nivel bajo de gravedad y no ponían en riesgo al sistema informático.

### ***3.4 Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IEEPCO***

Las actividades de esta línea de trabajo se realizaron desde el inicio del mes de mayo y se concluyeron el día miércoles 22 de mayo de 2024 con una prueba que



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**

**Unidad Iztapalapa**

se apoyó en los servicios de una empresa que proporciona una plataforma tecnológica para este tipo de pruebas de seguridad.

Se realizaron las pruebas de acuerdo con las especificaciones indicadas en el Anexo Técnico del Convenio de Colaboración y se comprobó que los mecanismos de protección del PREP 2024 funcionaron de manera adecuada.

Las pruebas se aplicaron al portal de publicación de resultados del PREP y al portal principal del IEEPCO. Las pruebas realizadas no identificaron hallazgos.

Las pruebas realizadas no generaron evidencia de vulnerabilidades, por el contrario, mostraron que los mecanismos de defensa de la infraestructura se comportan como es esperado. En conclusión, la infraestructura es capaz de resistir ataques con las características de las pruebas realizadas.

#### **4. Conclusiones**

Con base a las pruebas y análisis realizados durante la auditoría, se concluye que el sistema informático y su infraestructura tecnológica realiza correctamente las funciones especificadas para registrar las actas de escrutinio y a partir de ellas generar los resultados de las distintas elecciones que se realizarán el 2 de junio.

Adicionalmente se concluye que el sistema informático del PREP y su infraestructura tecnológica es seguro y capaz de resistir ataques informáticos sin que su operación continua se vea afectada.