CONAHCYT
CONSEJO NACIONAL DE HUMANIDADES CIENCIAS Y TECNOLOGÍAS

CIMAT

2024
Felipe Carrillo
PUERTO
BENEMÉRITO DEL PROLETARIADO, REVOLUCIONARIO Y DEFENSOR DEL MAYAB

Entregable

Auditoría PREP 2024 - IEEG

Informe de Auditoría

Versión 1.0

Guanajuato, Gto., 31 de mayo de 2024

CONAHCYT
CONSEJO NACIONAL DE HUMANIDADES CIENCIAS Y TECNOLOGÍAS

CIMAT

2024
Felipe Carrillo PUERTO
BENEMÉRITO DEL PROLETARIADO, REVOLUCIONARIO Y DEFENSOR DEL MAYAB

Contenido

1. Equipo auditor

Nombre
Ing. Ma. Guadalupe Aguilar Valtierra
Mtro. Juan José Castro Ceballos
Ing. Juan Esteban González Armas
Ing. Ulises Andrés Martínez Rodríguez
Dr. Jezreel Mejía Miranda
Dra. Mirna Ariadna Muñoz Mata
Mtro. José Ramón Pérez Villarreal
Mtro. Juan Luis Salazar Villanueva (Líder del equipo auditor)

2. Introducción

De acuerdo a lo dispuesto en la normativa del Reglamento de Elecciones del INE (RE), en su Artículo 346, se indica que el Instituto y el Organismo Público Local (OPL), deberán implementar un sistema informático para la operación del PREP, el cual deberá contemplar las etapas mínimas del Proceso Técnico Operativo (PTO), señaladas en el anexo 13 de este Reglamento. Así mismo, el Reglamento estipula en su Artículo 347 que el Instituto y los OPL deberán someter su sistema informático a una auditoría técnica para la cual se deberá designar un ente auditor que lleve a cabo la auditoría del PREP. El Anexo 13 del Reglamento, en su Capítulo III, estipula que "La auditoría de verificación y análisis del sistema informático que será utilizado en la implementación y operación del PREP, se deberá realizar con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados conforme a la normativa aplicable y vigente".

El alcance de la auditoría deberá cubrir, como mínimo, los puntos siguientes:

- Pruebas funcionales de caja negra al sistema informático para evaluar la integridad en el procesamiento de la información y la generación de resultados electorales preliminares.
- Análisis de vulnerabilidades, considerando al menos pruebas de penetración y revisión de configuraciones a la infraestructura tecnológica del PREP.

En cumplimiento de los términos de la normativa descritos anteriormente, el Instituto Electoral del Estado de Guanajuato (IEEG) a través de la Unidad Técnica de Sistemas de Información y Telecomunicaciones (UTSIT), ha dispuesto un Sistema Informático del PREP (SIPREP) para las elecciones a celebrarse el día 2 de junio de 2024, y ha conferido la tarea del ente auditor al Centro de Investigación en Matemáticas, A. C. (CIMAT).

Los trabajos de auditoría al Sistema Informático e Infraestructura Tecnológica del PREP para el Proceso Electoral 2023-2024 en el estado de Guanajuato se realizarán conforme el "Anexo Técnico para la contratación del ente auditor del Programa de Resultados Electorales Preliminares" que se basa en la normatividad electoral vigente para estos trabajos.

Las líneas de trabajo que se consideran son:

1. Pruebas funcionales de caja negra al sistema informático del PREP (SIPREP) y a la aplicación que se utilizarán para operar el mecanismo de digitalización de las Actas desde las casillas, para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares.

2. Análisis de vulnerabilidades, considerando al menos pruebas de penetración y revisión de configuraciones a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP.
3. Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IEEG.
4. Validación del sistema informático del PREP y de sus bases de datos, ante un tercero con fe pública.

1. Pruebas funcionales de caja negra al SIPREP

- Analizar el funcionamiento del SIPREP, en relación con las fases del Proceso Técnico Operativo (PTO), considerando al menos, la digitalización, captura de datos, verificación y publicación de resultados, mediante flujos completos e interacción entre los diversos módulos desde digitalización en la casilla, acopio, digitalización en CATD, captura y verificación de datos, así como la publicación de resultados y el cotejo.
- Analizar el funcionamiento del aplicativo desarrollado para la digitalización de las Actas desde las casillas, y, en su caso, la captura de datos desde las casillas. Dicho análisis se hará mediante flujos completos e interacción entre los diversos módulos y fases del PTO.
- Verificar el cumplimiento de las especificaciones funcionales y los requerimientos contenidos en la documentación técnica y normatividad aplicable que será proporcionada por el IEEG.
- Verificar la correspondencia de la captura de los datos plasmados en las Actas PREP con los presentados en la publicación, mediante los distintos tipos de reportes desplegados por el PREP, considerando datos, imágenes y bases de datos.

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

- Identificar debilidades de seguridad en la infraestructura y servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP mediante la ejecución de pruebas de penetración y revisión de configuraciones de seguridad.
- Clasificar el impacto y documentar las vulnerabilidades identificadas con el propósito de recomendar al IEEG las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.

- Verificar que las medidas implementadas por el IEEG hayan atendido adecuadamente las vulnerabilidades reportadas.
- Verificar la implementación de un sistema de rollback que permita revertir los cambios a la versión anterior en caso de ser necesario, así como asegurar la implementación de un sistema de backup y restauración en caso de ser necesario.

3. **Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IEEG**

   Dichas pruebas de negación de servicio deberán considerar dos apartados:

   - Tráfico no malintencionado, que consiste en transacciones sintéticas que simulen el tráfico legítimo que se espera el día de la Jornada Electoral.
   - Tráfico de red malintencionado, consistente en paquetes de red malformados.

4. **Validación del SIPREP, así como de sus bases de datos**

   Se verificará que los programas auditados se encuentren operando desde el inicio y hasta el cierre de operación del PREP y que las bases de datos se encuentren debidamente inicializadas

3. Actividades realizadas

2.1 Descripción

1. **Pruebas funcionales de caja negra al SIPREP.**
   La metodología que se siguió se tomaron como base los estándares ISO/IEC 29110-5-1-2, el ISO/IEC/IEEE 29119-2, el ISO/IEC/IEEE 29119-3 y el ISO/IEC/IEEE 29119-4 con la finalidad de seguir un conjunto de buenas prácticas de estándares internacionales.

   Para la construcción de los casos de prueba se utilizaron las siguientes técnicas: pruebas de casos de uso, pruebas de diagramas de flujo, transición entre estados, pruebas de funcionamiento, particiones de equivalencia y análisis de valores límite.

   En total se construyeron y evaluaron un total de 107 casos de prueba en dos iteraciones.

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

   Para esta línea de auditoría se tomaron como base las recomendaciones de: OWASP (Open Web Application Security Project), CIS Controls (Center for Internet Security - Controls), AWS Security Hub y la ISO/IEC 27000.

   Teniendo un total de 126 controles de validación que se evaluaron en dos iteraciones.

3. **Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IEEG.**

   En esta línea se realizaron las pruebas de negación de servicios al sitio de publicación del PREP conforme el anexo técnico del ente auditor.

   - Al menos 20 Gbps de throughput.
   - Al menos se ejecutará: DNS QUERY FLOOD, SLOWLORIS Attack, CACHE-BUSTING, HTTP FLOOD.

4. **Validación del SIPREP, así como de sus bases de datos.**

   Se desarrollarán los scripts para obtener la huella criptográfica SHA-256 empleadas en la validación del esquema de la base de datos y de los aplicativos utilizados en los procesos del PREP.

La ejecución del proceso de validación se ejecutará en 3 momentos claves:

1. Previo a la jornada electoral (1 de junio)
2. Al inicio a la jornada electoral (2 de junio)
3. Al cierre de la jornada electoral y pasado el último corte del sitio de publicación PREP. El día 3 de junio después de las 19:00 horas.

El detalle de los hallazgos encontrados, recomendaciones emitidas y su atención a estas se encuentran de manera extensa en la documentación entregada al IEEG conforme la tabla del siguiente punto.

2.2 Documentación entregada

Línea de trabajo	Documento
Pruebas funcionales de caja negra al SIPREP	Plan de pruebas funcionales de caja negra del sistema informático y/o servicios relacionados con Tecnologías de la Información y Comunicaciones
	Informe preliminar de las pruebas funcionales de caja negra del sistema informático y/o servicios relacionados con Tecnologías de la Información y Comunicaciones
	Informe sobre la ejecución de la prueba funcional
	Informe final de las pruebas funcionales de caja negra del sistema informático y/o servicios relacionados con Tecnologías de la Información y Comunicaciones
Análisis de vulnerabilidades a la infraestructura y servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP	Plan de pruebas de penetración a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP
	Informe preliminar de las pruebas de penetración a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP

	Informe de la aplicación de recomendaciones de las pruebas de penetración a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP.
	Plan de revisión de configuraciones de la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP
	Informe preliminar de la revisión de configuraciones de la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP
	Informe de la aplicación de recomendaciones de la revisión de configuraciones de la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP
	Informe final del análisis de vulnerabilidades a la infraestructura tecnológica y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP
Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IEEG	Plan de trabajo detallado
	Plan de ataques de negación de servicio
	Informe de resultado
	Estadísticas del tráfico de red generado
Validación del SIPREP, así como de sus bases de datos	Plan de trabajo detallado

	Procedimiento técnico con el esquema de validación de los componentes, programas y configuraciones auditadas; y de las bases de datos del sistema informático del PREP

De acuerdo a la normativa del INE, el IEEG ha realizado 3 simulacros, de los cuales el ente auditor ha estado como observador y entregado informes. Dentro de las actividades de la "Validación del SIPREP, así como de sus bases de datos" se realizarán las actividades de generación de huella criptográfica y se emitirán las constancias de hechos avaladas por un notario público. Finalmente, posterior a la jornada electoral se emitirán informes de desempeño.

Lo anterior se muestra en la siguiente tabla:

Documento	Estado del documento
Informe del primer simulacro	Entregado
Informe del segundo simulacro	Entregado
Informe del tercer simulacro	Entregado
Constancia de hechos de la generación de huellas criptográficas de los componentes, programas y configuraciones auditadas del sistema informático PREP	Pendiente (1 de junio)
Constancias de hechos de la validación de los componentes, programas y configuraciones; y de las bases de datos del sistema informático PREP.	Pendiente (2 de junio)
Informe de desempeño de la operación del sistema informático y/o servicios relacionados con Tecnologías de la Información y Comunicaciones	Pendiente (14 de junio)
Informe de desempeño de la operación del sistema informático respecto a la infraestructura tecnológica y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP	Pendiente (30 de junio)

4. Dictamen

Con base a la auditoría realizada entre el 1 de marzo y el 31 de mayo del 2024 sobre el Sistema Informático PREP en el alcance explicado en el documento. El ente auditor hace constar que:

1) El sistema informático del PREP cumple con los requerimientos funcionales y se apega al Proceso Técnico Operativo, el Anexo 18.5 del Reglamento de Elecciones, el Manual de Manejo de Inconsistencias en las Actas PREP para el Proceso Electoral Local 2023 - 2024 y la implementación de las plantillas proporcionadas por el INE para el sitio de publicación del PREP.
2) Se han implementado y verificado diferentes mecanismos para asegurar que la infraestructura tecnológica: servidores, equipo de red, laptop, equipos de escritorio, equipos celulares se encuentren operando correctamente y estén libres de las vulnerabilidades más conocidas.
3) Se cuenta con equipo para asegurar la continuidad debido a una falla eléctrica o falla en el proveedor de internet.
4) Se han realizado pruebas y verificado que el sitio de publicación de resultados del PREP soporta millones de peticiones malintencionadas con la finalidad de hacer una negación de servicios. Esto gracias a la infraestructura que soporta el sitio de publicación PREP y que se han implementado diferentes herramientas y configuraciones robustas.
5) Se cuenta con un procedimiento técnico que permite validar que los aplicativos auditados corresponden a los que se utilizarán en la jornada electoral del 2 de junio del 2024.
6) Se realizó un estudio y se cuenta con un procedimiento técnico para verificar el estado que debe tener la Base de Datos y las tablas que deben estar vacías previó al arranque del PREP.
7) Durante los ejercicios de los simulacros se observó que los aplicativos, infraestructura física y tecnológica del sistema PREP se desempeñan bien con una carga similar a la esperada en la jornada electoral. Cabe mencionar que en los últimos dos simulacros se alcanzó el 100% de captura de actas.

El presente informe se emite en la ciudad de Guanajuato, Gto., a 31 de mayo del 2024.

Mtro. Juan Luis Salazar Villanueva
Líder del equipo auditor PREP 2023-2024
Centro de Investigación en Matemáticas (CIMAT)