Universidad Nacional Autónoma de México
Facultad de Estudios Superiores Aragón
Centro Tecnológico Aragón
Laboratorio de Cómputo

Auditoría Informática al Programa de Resultados Electorales Preliminares PREP 2025 para el Instituto Electoral del Estado de Puebla

Informe Final de la Auditoría al Sistema PREP 2025

Periodo de evaluación:

del 4 de febrero al 20 de marzo de 2025

Bitácora de modificaciones

Historia de versiones

Versión	Fecha	Descripción del cambio	Autor
0.1.0	04/febrero/2025	Creación del formato.	Paulett Jaqueline Toledo Varela
0.2.0	10/febrero/2025	Estructuración Rubros	Yazmin Yanela Santiago Gutiérrez, Emiliano Contreras Padilla
0.4.0	17/febrero/2025	Pruebas funcionales de caja negra	Axel Pantoja Romo, Paulett Toledo Varela, Diego Rocha Zamudio, Atziri Sireth Cruz Mejia
0.6.0	20/febrero/2025	Análisis de vulnerabilidades a la infraestructura tecnológica	Luis Fernando Lira Guzmán, Rafael Hernández Vega
0.8.0	15/marzo/2025	Validación del sistema informático del PREP y de sus bases de datos	Fernando Lira Guzmán
0.9.0	18/marzo/2025	Pruebas de denegación de servicio	Yazmin Yanela Santiago Gutiérrez
1.0.0	18/marzo/2025	1era Revisión	Edgar Mórales Palafox
1.1.0	19/marzo/2025	2da. Revisión	Jesús Hernández Cabrera
1.2.0	19/marzo/2025	Revisión final	Marcelo Pérez Medel

Contenido

1. OBJETIVO GENERAL

Realizar una auditoría informática al Programa de Resultados Electorales Preliminares (PREP) de las elecciones 2025, del Instituto Electoral del Estado de Puebla (IEE Puebla) conforme al reglamento de elecciones aprobado mediante acuerdo del Consejo General del Instituto Nacional Electoral. No. INE/CG661/2016.

De forma general, la auditoría deberá determinar si el sistema del PREP es seguro, robusto, confiable y realiza exclusivamente las operaciones y funciones para las cuales fue diseñado, de acuerdo con el manual de usuario, garantizando la integridad en el procesamiento de toda la información.

2. OBJETIVOS ESPECÍFICOS

A. Revisar el sistema informático y los correspondientes aplicativos desarrollados específicamente para el PREP en términos de funcionalidad. La auditoría deberá determinar que los aplicativos PREP, realizan las funciones descritas en el manual de usuario y solamente esas, es decir, que el programa hace lo que se espera de él, procesando transparente y correctamente la información desde su origen hasta la publicación.

   Dentro de los aspectos a revisar en el rubro de calidad del sistema se incluyen:

   - Verificación de la arquitectura del sistema.
   - Controles adecuados en la entrada de datos.
   - Almacenamiento y restauración de datos.
   - Implementación de bitácoras en el procesamiento de datos sensibles.
   - Manejo de errores.
   - Evaluación del desempeño de los recursos.

B. Probar todos los aplicativos desarrollados específicamente para el **PREP**, en términos de funcionalidad.

C. Analizar las posibles vulnerabilidades de la infraestructura tecnológica del **PREP**.

D. Ejecutar pruebas de denegación de servicios, de inyección de código malicioso y de acceso a los diversos recursos del sistema informático.

E. Diseñar y ejecutar pruebas de Penetración (PenTest) al sistema e infraestructura que soporta al sistema PREP.

3. ALCANCES

A. La auditoría se realiza del 04 de febrero al 21 de marzo de 2025.

B. La auditoría consiste en dos partes: la primera, corresponde a la revisión de la funcionalidad y la segunda, a la identificación de posibles vulnerabilidades que tenga el sistema.

C. Realizar una planificación de la auditoría, identificando claramente los recursos materiales y técnicos necesarios para llevarla a cabo; dicha planificación se encuentra en poder de la Unidad Técnica de Servicios Informáticos.

D. Efectuar la auditoría con base a los requerimientos establecidos en el anexo técnico del convenio de colaboración UNAM – IEE Puebla y en la metodología IEEE Std 1028™-2008 “IEEE Standard for Software Reviews and Audits” la cual es una metodología estandarizada internacionalmente.

4. METODOLOGÍA

La metodología utilizada para la realización de esta auditoría es la IEEE Std 1028™-2008 “IEEE Standard for Software Reviews and Audits”, la cual es una metodología estandarizada internacionalmente y se utilizó para la realización de las pruebas OSSTMM, que es un estándar para la realización de pruebas y métricas de seguridad desarrollado por un grupo de profesionales especialistas en seguridad informática y agrupados bajo una organización denominada ISECOM (Institute for Security and Open Methodologies), OSSTMM, hace referencia al manual o documento guía de OSSTMM, OSSTMM Manual (en inglés). Los casos de pruebas del OSSTMM se agrupan en cinco (5) diferentes áreas que en conjunto prueban:

A. Robustez de los controles implementados para la seguridad de la información y de los datos.
B. Los controles implementados para la infraestructura de cómputo y de comunicaciones, de redes inalámbricas y dispositivos móviles.
C. Los controles para la detección de intentos de ataques de ingeniería social.
D. Los niveles de concientización relacionados a los temas de seguridad informática en el personal de una organización.
E. Los controles de seguridad física de una organización.

En este servicio, la metodología OSSTMM v3 se usó exclusivamente para delinear las actividades técnicas de los diferentes elementos a ser probados y las acciones a realizar antes, durante y después de cada una de las pruebas. La metodología OSSTMM contempla de manera general las siguientes fases de estudio:

- Definición de Objetivos.
- Exploración.
- Enumeración.
- Explotación.
- Escalación y finalización de prueba.

Otro estándar utilizado fue OWASP (www.owasp.org), el cual es una metodología que contiene información de cómo construir un ambiente de pruebas y del tipo de técnicas de verificación que se deben usar en los desarrollos de aplicaciones WEB. Teniendo como objetivo principal el desarrollo de aplicaciones seguras.

En este documento se mencionan cada una de las pruebas que exige la metodología OWASP, como parte de una lista de verificación de las tareas a llevar a cabo aplicando esta metodología. El objetivo es tener una matriz de pruebas/evaluaciones para determinar el grado de seguridad que presentan las aplicaciones desarrolladas. Las pruebas/evaluaciones pueden ser realizadas y/o complementadas a través de una serie de entrevistas, con esto se determina de manera adecuada el grado de madurez y la seguridad implícita en las aplicaciones desarrolladas internamente.

En resumen, lo que se debe hacer es lo siguiente:

- Recopilar información de las aplicaciones, infraestructura y entorno web.
- Examinar cada fase del proceso para probar vulnerabilidades.
- Identificar puntos críticos y atacarlos para determinar puntos de falla.
- Probar con diferentes métodos de ataque, de acuerdo con el checklist.
- Generar resultados.

5. RESULTADOS DE LA AUDITORÍA

Durante la realización de la auditoría, el equipo auditor se abstuvo de:

- Instalar cualquier tipo de puerta trasera o aplicación que permitiera acceso remoto encubierto y reiterado.
- Instalar cualquier tipo de keylogger, boot, troyano, rootkit o tecnología similar.
- Instalar aplicaciones de acceso remoto que sean claramente identificables como procesos activos y cuyos puertos, y conexiones sean visibles.
- Borrar, alterar o apagar el uso de las bitácoras (logs) en cualquier dispositivo, estación de trabajo o servidor.
- Modificar la configuración de un servidor, estación de trabajo o dispositivo de red.

Una vez concluida la auditoría, el equipo auditor no dejó ninguna modificación o rastro en la infraestructura del IEE Puebla originado a raíz de las pruebas realizadas.

Los resultados se muestran en las siguientes páginas:

A) Pruebas funcionales de caja negra al sistema informático del PREP.

Introducción

Esta sección contiene los resultados de las pruebas funcionales de caja negra, los cuales se obtuvieron al verificar el proceso técnico operativo mediante el PREP y PREP Casilla. Para lo cual, se consideran los lineamientos Operativos del Programa de Resultados Electorales Preliminares 2025; de dicho documento se toman en cuenta:

- Título II, Capítulo II, artículo 4.
- Título II, Capítulo III, artículo 5.
- Título II, Capítulo V, articulo 15.

De acuerdo con el plan de pruebas funcionales de caja negra, se verifica el ciclo de vida del sistema PREP y PREP Casilla. Estos deben cumplir mínimo con las etapas: Análisis, Diseño, Construcción y Pruebas.

De acuerdo con el plan de pruebas funcionales de caja negra, la ejecución de casos de prueba se realizó del 04 al 26 de febrero de 2025 (incluyendo las pruebas realizadas en presencia del INE).

Metodología

Se hace uso de OWASP (www.owasp.org), la cual es una metodología que contiene información de cómo construir un ambiente de pruebas y del tipo de técnicas de verificación que se deben usar en los desarrollos de aplicaciones WEB, teniendo como objetivo principal el desarrollo de aplicaciones seguras y en la metodología IEEE Std 1028™-2008 “IEEE Standard for Software Reviews and Audits”.

La metodología empleada para la ejecución de las pruebas funcionales de caja negra está fundamentada en el diseño de casos de prueba para los diferentes casos de uso relacionados con el sistema, tomando como base la documentación proporcionada por los equipos de desarrollo del sistema PREP.

El formato utilizado para registrar los casos de prueba se muestra en la Ilustración siguiente:

	Proyecto:	Auditoría PREP 2025 IEE Puebla	
	Institución:	Universidad Nacional Autónoma de México Facultad de Estudios Superiores Aragón Centro Tecnológico Aragón	
No Caso de prueba:	06	Nombre:	Digitalización de acta sin conexión mediante la aplicación móvil.

Diseñado por:	Axel Jesús Pantoja Romo.
Probado por:	
Fecha de la prueba:	
Tipo de prueba:	Software.
Precondiciones:	Tener acceso a la aplicación móvil "PREP APP" y haber ejecutado alguno de los casos de prueba "Identificación de acta por código QR" o "Identificación manual de acta". Contar con un acta disponible para digitalización.
Descripción de la prueba:	Se verificarán los flujos principales del caso de uso para realizar la digitalización de actas mediante la aplicación móvil "PREP APP" cuando no se tiene conexión a internet.

Elemento (s) a ser probado	
1	Corroborar el correcto funcionamiento de la aplicación móvil cuando se pierde la conexión al digitalizar un acta.
2	Verificar el funcionamiento del botón de sincronización de actas pendientes.

Configuración de la prueba (hardware, software, base de datos, tiempo)

Hardware: Dispositivo Android con acceso a internet y a sus configuraciones para desactivar la conexión.

Software: Aplicación móvil "PREP APP".

Base de datos: Se requiere un usuario con privilegios de sólo lectura.

Especificaciones

Entrada	Resultado esperado	Resultado obtenido
-Realizar la identificación de un acta con la aplicación móvil.	-Visualización de un botón para cada tipo de elección.	
-Desactivar la conexión a internet del dispositivo.	-No se espera respuesta por parte de la aplicación.	
-Presionar el botón del tipo de elección del acta.	-Se muestra la cámara del dispositivo con el botón de captura deshabilitado mientras la imagen no se enfoque.	
-Mantener la cámara estable para permitir el enfoque.	-El botón de captura se habilita.	
-Presionar el botón de captura.	-Se toma una fotografía y se muestra la pantalla de recorte.	
-Mover las guías y presionar el	-Se muestra la imagen recortada según la	

Formato de casos de prueba

Resultados

En el presente documento se describe la información correspondiente a los siguientes rubros: Documentación técnica, Revisión del sistema y Hallazgos.

	Documentos solicitados	No aplica	Entregados	No entregado
PROISI	21	0	21	0
IEE Puebla	2	0	2	0

Las pruebas de funcionalidad se realizaron a través de 58 casos de prueba, en ellos se establecen los flujos principales del funcionamiento técnico operativo del sistema PREP. Cada caso de prueba contiene un número de pasos que tienen que ser revisados, para dichas pruebas se estableció un total de 737 pasos, los cuales resultan en un estatus:

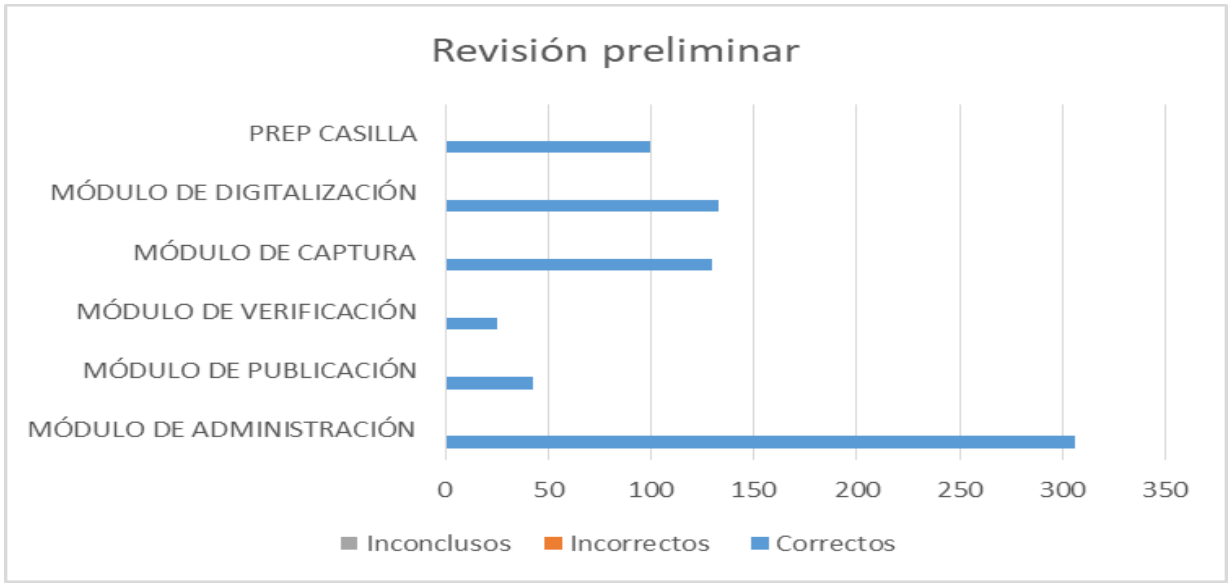
- Correcto. - Al ejecutar el paso, el resultado obtenido es igual al resultado esperado.
- Incorrecto. - Se ejecuta el paso y el resultado obtenido es distinto al esperado.
- Inconcluso. - Se ejecuta el paso, sin embargo, por falta de información en Base de Datos no se puede observar el resultado para compararlo con lo esperado.

A continuación, se presenta la información obtenida en la ejecución de los casos de prueba para el sistema PREP durante las dos etapas de revisión (Preliminar y final), así como los hallazgos encontrados.

Resultados de la revisión preliminar:

En la siguiente tabla de la primera revisión del flujo de operación, podemos observar que, en relación con los casos de prueba ejecutados, el sistema respondió en su mayoría adecuadamente, sin embargo, hubo algunos puntos a superar para la segunda revisión.

	Pasos a probar	Correctos	Incorrectos	Inconclusos
PREP Casilla	100	100	0	0
Módulo de digitalización	133	133	0	0
Módulo de captura	130	130	0	0
Módulo de verificación	25	25	0	0
Módulo de publicación	43	43	0	0
Módulo de administración	306	306	0	0
Total	737	737	0	0

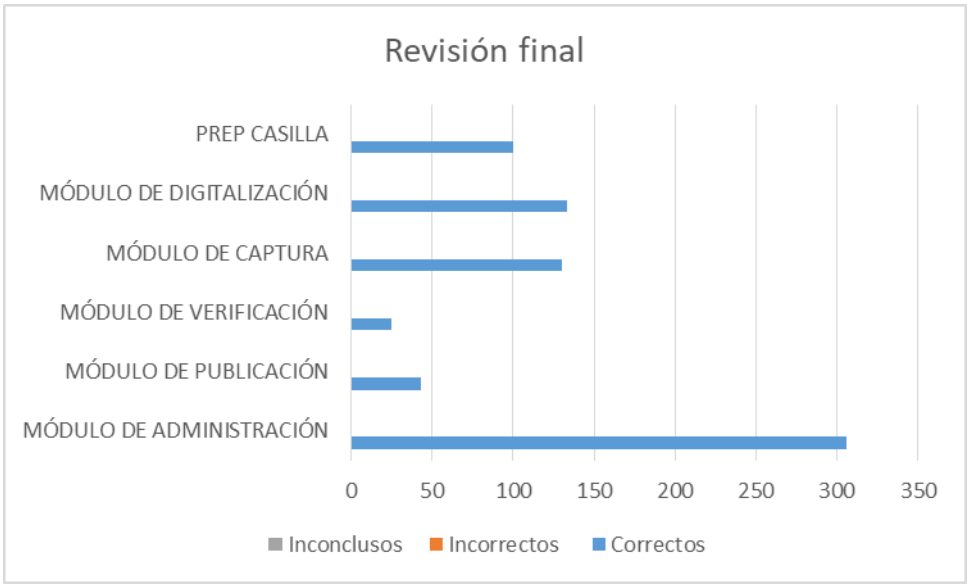


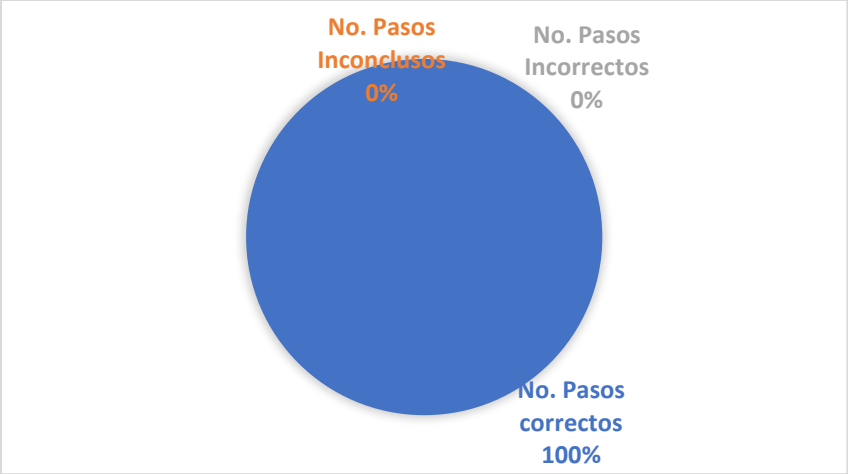
Resultados de la revisión final:

En la revisión final, confirmamos los resultados obtenidos durante la revisión preliminar, manteniendo el 100% de efectividad con 737 pasos correctos, 0 incorrectos y 0 inconclusos. Es importante destacar que el sistema funcionó de manera óptima desde el inicio, demostrando un alto nivel de calidad en su implementación. Aunque se señalaron algunas recomendaciones en el informe preliminar para el sitio de publicación, estas fueron de carácter preventivo y no afectaban la funcionalidad esencial del sistema. Se dará seguimiento a estos aspectos durante

la ejecución del sistema el día de la jornada electoral, aunque no representan riesgos para la operación.

	Pasos a probar	Correctos	Incorrectos	Inconclusos
PREP Casilla	100	100	0	0
Módulo de digitalización	133	133	0	0
Módulo de captura	130	130	0	0
Módulo de verificación	25	25	0	0
Módulo de publicación	43	43	0	0
Módulo de administración	306	306	0	0
Total	737	737	0	0





Como parte de las pruebas, se realizó un corte de energía durante el ejercicio de simulacro, en el cual se pudo observar que cuentan con planta de energía que se activa de forma manual y UPS conectados a las PCS y escáneres que entran de forma automática mientras se estabiliza la planta. Para la parte de conectividad se cuentan con dos proveedores de Internet, los cuales están conectados simultáneamente con el propósito que, si se cae un enlace, el otro continúa dando servicio sin interrumpir el acceso a Internet.

Adicionalmente, durante las pruebas funcionales se reportaron dos hallazgos, uno respecto al ciclo de vida y otro al proceso técnico operativo del sistema; mismos que muestran resumidos a continuación:

	Hallazgo
6.1. Ciclo de vida	Para la documentación generada durante las distintas fases del ciclo de vida del sistema PREP, se recomienda generarla con mejor nivel de detalle.
6.2. Proceso técnico operativo	Para PREP Casilla se recomienda contar con una base fija con luz para tener un mejor enfoque del acta.

Durante el primer simulacro se realizaron pruebas de conectividad. La inicial consistió en desconectar uno de los dos proveedores de servicio de internet (ISP), del router localizado en el CCV. El sistema se mantuvo en equilibrio y en ningún momento se notó la desconexión de manera visible. Todo el CCV continúo con sus operaciones de forma normal.

Servidor de conectividad a la red

Desconexión del primer canal de salida de Internet

Desconexión del segundo canal de internet

B) Validación del sistema informático del PREP y de sus bases de datos.

Objetivo

Validar que el sistema informático del PREP que operará el día de la Jornada Electoral, corresponda al software auditado, así como que la base de datos se encuentre sin registros adicionales a los necesarios para que el sistema opere. La validación respecto a la

correspondencia del software auditado y el utilizado en la operación del PREP, se tendrá que realizar al inicio, durante y al final de la operación del sistema informático del PREP.

Alcance

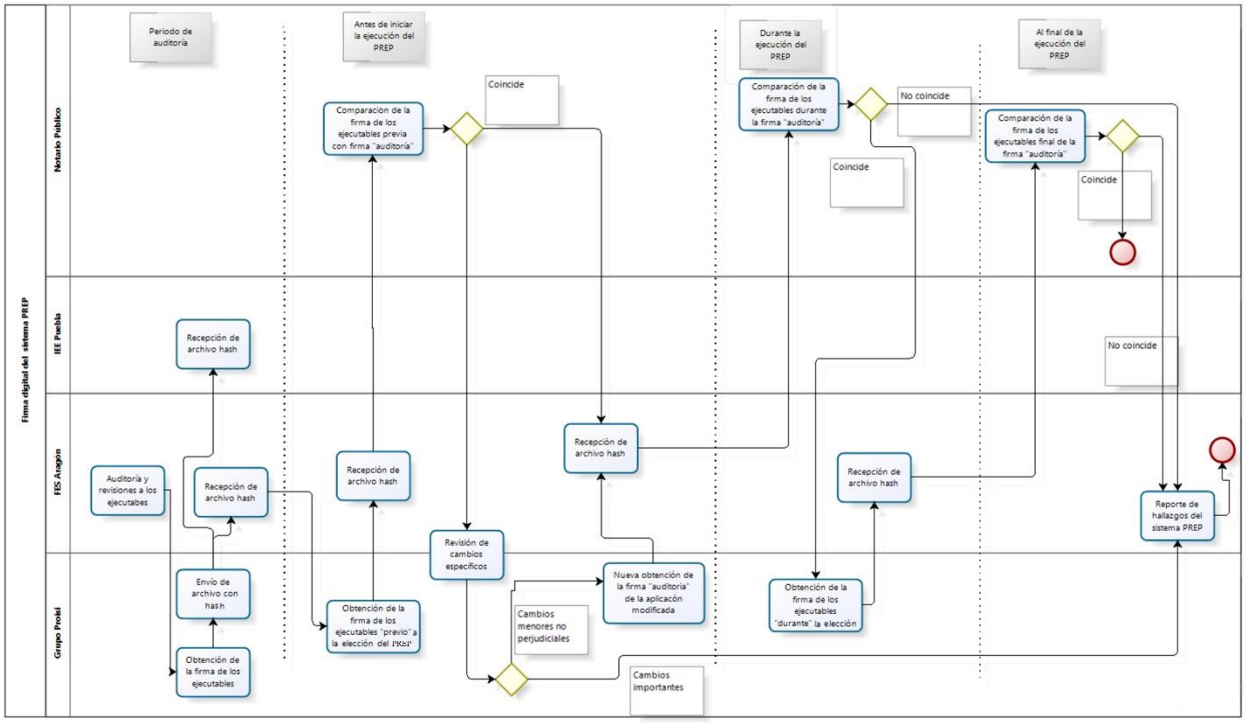
Llevar a cabo un procedimiento técnico para verificar que los programas auditados se encuentren operando desde el inicio y hasta el cierre de operación del sistema informático del PREP, así como que la base de datos se encuentre debidamente inicializada.

Procedimiento técnico

De acuerdo con los lineamientos, el procedimiento para la validación del sistema PREP consistirá en aplicarle una función hash SHA-256 a los archivos que lo componen, antes del día de las elecciones, lo cual dará como resultado un valor único que posteriormente será comparado con las cadenas alfanuméricas que se generarán bajo el mismo procedimiento, al inicio, durante y al finalizar la ejecución del sistema.

Para el caso de las bases de datos, se ejecutarán las consultas necesarias para verificar que no contengan registro alguno, previo al arranque del sistema.

El procedimiento de firma se detalla en el siguiente diagrama:



Procedimiento de validación del sistema informático.

C) Análisis de vulnerabilidades a la infraestructura tecnológica.

Objetivos

- Identificar debilidades de seguridad en la infraestructura tecnológica, 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 Instituto Electoral del Estado de Puebla las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.
- Verificar que las medidas implementadas por el Instituto Electoral del Estado de Puebla hayan atendido adecuadamente las vulnerabilidades reportadas.

Alcance

El análisis de vulnerabilidades de la infraestructura tecnológica deberá realizarse con base en las etapas que se describen a continuación.

Pruebas de penetración (pentest). Las pruebas de penetración se deberán llevar a cabo tanto desde el interior, como desde el exterior de la red de datos a examinar y deberán enfocarse en:

- Servidores.
- Aplicaciones web.
- Equipos de telecomunicaciones.
- Estaciones de trabajo.

Pruebas de penetración (pentest)

Durante el análisis del sitio https://puebla-extra-sitio-2025.sistemaprep.com/, se reportó un solo hallazgo de nivel de criticidad media, se solicitó información para la remediación pero el equipo auditor no recibió respuesta alguna, por lo que el hallazgo persiste.

Durante las pruebas de penetración al sitio https://www.ieepuebla.org.mx reveló varias vulnerabilidades pero solo una de ellas considerada significativa con un nivel de importancia crítico, el cual fue reportado para su atención por parte del Instituto.

Antes de redactar este documento, y a solicitud del IEE Puebla, se realizó una nueva verificación para determinar si el hallazgo previamente identificado persistía en el sitio. Al repetir las pruebas, confirmamos que el hallazgo había sido resuelto.

Cabe mencionar que, en el contexto de protección contra ataques de penetración, la tecnología Cloudflare juega un papel crucial en la seguridad del sistema PREP del Estado de Puebla. Al actuar como un intermediario entre los usuarios y los servidores del sistema. Los dos sitios reportados en los párrafos anteriores implementan está solución como una capa adicional de seguridad.

Revisión de configuraciones

Durante la auditoría, examinamos exclusivamente las configuraciones de seguridad a las que se nos permitió acceso. Se nos otorgó acceso físico en el Centro de Captura y Verificación (CCV) y acceso parcial y de forma documental a la infraestructura en la nube, es importante destacar la falta de respuesta y marcada resistencia por parte del proveedor para colaborar en esta prueba y aprovechar la auditoría para ofrecer un servicio de mejora continua.

Durante la revisión documental se observó lo siguiente:

La infraestructura en la nube AWS revisada para el PREP ha sido adaptada para optimizar la seguridad, la disponibilidad y el rendimiento de los servicios que ofrece. Este sistema usa una organización eficiente de recursos en la nube, con subredes y grupos de seguridad que estructuran y protegen estos recursos. También incluye balanceadores de carga que ayudan a distribuir el tráfico de manera eficaz y aumentar la resistencia del sistema frente a posibles fallos.

Se han implementado múltiples firewalls para proteger diferentes niveles de la red, garantizando que solo el tráfico autorizado tenga acceso. Además, se usa el servicio de Cloudflare, que actúa como CDN, Firewall de Aplicación Web, y protector contra ataques de denegación de servicio, esencial para mantener el sistema operativo durante eventos importantes como las elecciones del 23 de marzo.

Las bases de datos y otros servicios críticos se distribuyen en múltiples zonas para garantizar su funcionamiento continuo, complementado con estrategias de replicación y redundancia de datos. La seguridad de los datos transmitidos se fortalece mediante certificados SSL/TLS y se menciona el uso de políticas de cifrado para los datos almacenados, aunque no se detallan herramientas específicas.

La infraestructura se monitorea continuamente a través de CloudWatch, facilitando una rápida respuesta ante cualquier incidente. Esto se complementa con políticas de gestión de registros y auditorías para mejorar la detección y resolución de problemas de seguridad.

En cuanto al Centro de Captura y Verificación (CCV) del PREP, se han realizado pruebas de seguridad y configuración de la red y dispositivos asociados, utilizando herramientas como Nessus para el escaneo de redes y pruebas detalladas en dispositivos clave. La red LAN en el CCV ha sido evaluada y confirmada como segura tras la remedición de dos hallazgos reportados, remediación que fue documentada y reportada al equipo auditor. El centro de captura también cuenta con medidas de respuesta ante cortes de energía y proveedores de internet redundantes para asegurar la continuidad operativa.

Las configuraciones del firmware en dispositivos específicos como el router empleado incluye varias medidas de seguridad para proteger la red local y la gestión de usuarios, como reglas de firewall y bloqueos contra ataques de denegación de servicio (DoS), garantizando una gestión segura y controlada por un administrador designado.

D) Pruebas de denegación de servicio.

Objetivo

Realizar ataques de denegación de servicio que permitan identificar y evaluar deficiencias en el sistema y posteriormente, aplicar las medidas necesarias para asegurar la correcta y continua disponibilidad del servicio Web de los sitios de publicación de resultados del PREP 2025 y del sitio principal del IEE Puebla, durante el periodo de operación del PREP 2025.

Documentar los hallazgos detectados durante la realización de las pruebas de denegación de servicio.

Alcance

Generar tráfico de red desde la infraestructura del ente auditor, o en su caso la que éste determine. Para los casos en que el software del PREP, sea aprovisionado a través de una nube pública, se deberá considerar un proveedor autorizado de acuerdo con lo establecido por cada proveedor de nube, hacia los servicios web que se publican dentro del dominio del Instituto

Electoral del Estado de Puebla (IEE), ya sea en su propia infraestructura o en la que provea un tercero.

Se debe tener en consideración que el tráfico generado deberá ejecutarse tomando en consideración si el software del PREP se encuentra desplegado en ambiente de tipo on-premise o servicio de nube pública.

Las pruebas de denegación 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.

Pruebas

Las pruebas consistieron en las siguientes fases.

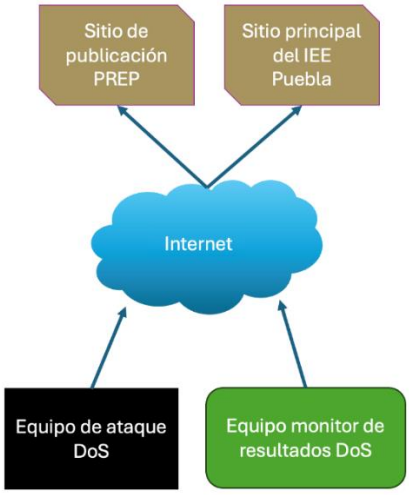
Fase de preparación. - El objetivo de esta fase es la identificación de objetivos y la configuración de las herramientas utilizadas para la prueba.

Fase de ataque. - En esta fase se ejecutaron las herramientas para realizar un ataque DoS.

- Fase 1.- Se realiza un ataque moderado en ancho de banda y orientado más al ataque lógico a protocolos (TCP, UDP, ICMP y capa de aplicación) y simulando carga de trabajo de usuarios legítimos usando la herramienta JMeter.
- Fase 2.- En esta fase se incluyen las herramientas de la etapa 1, herramientas volumétricas y adicionalmente, equipos de Red UNAM para generar un mayor impacto al sistema.

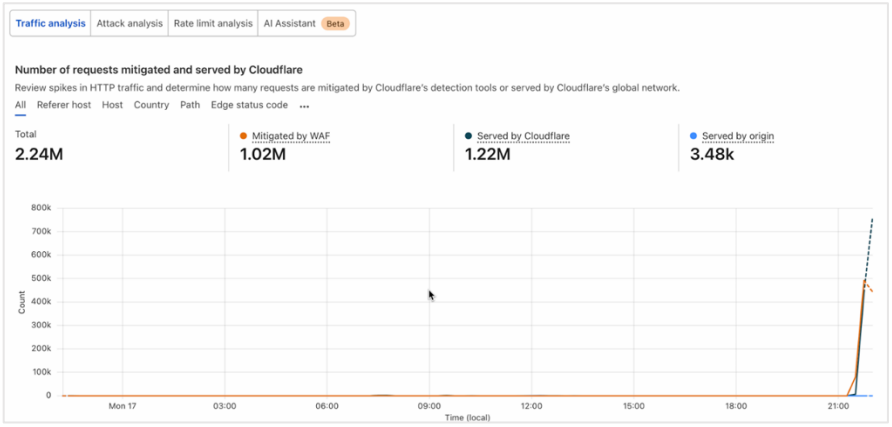
Organización del equipo de seguridad.

Las pruebas fueron ejecutadas por el equipo auditor de seguridad, desde puntos diferentes en Internet, un miembro del equipo realizó operaciones de monitoreo y también participó con el resto del equipo para la ejecución del ataque de manera simultánea.

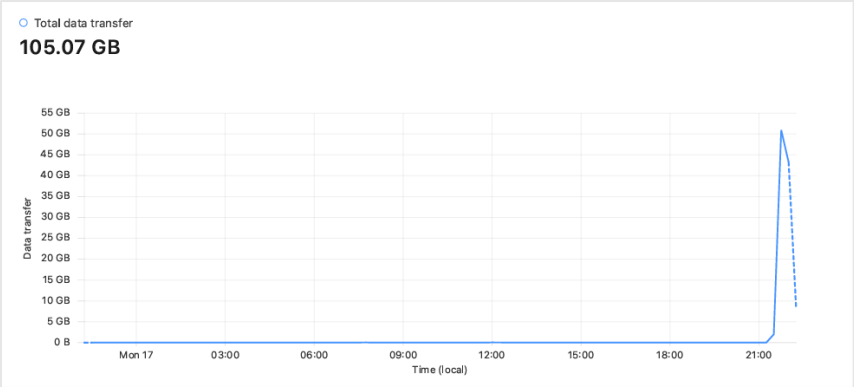


Resultados

El sitio PREP Puebla 2025: https://puebla-extra-sitio-2025.sistemaprep.com/ superó exitosamente la prueba, a continuación se describen los resultados.



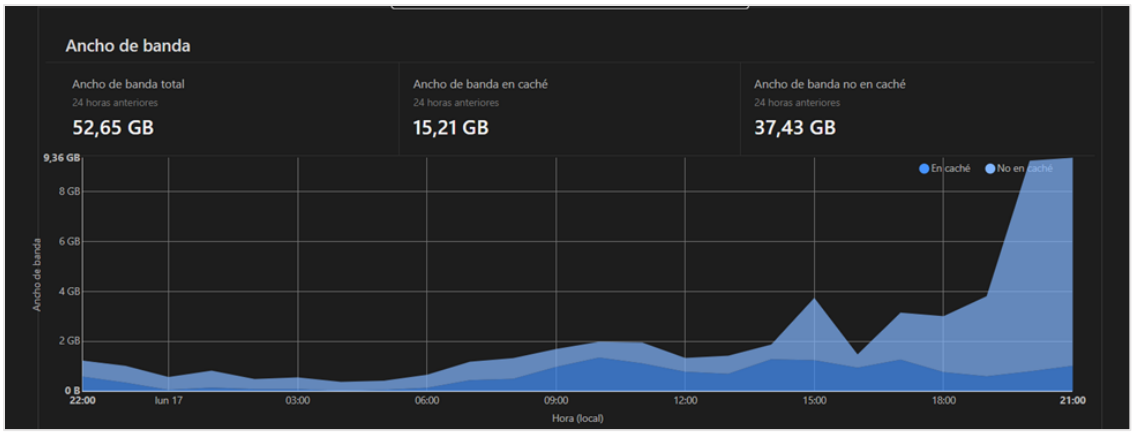
Como se puede observar en la imagen anterior se muestra el resumen del reporte del WAF, con un total de 2.24 millones de peticiones realizadas al sitio, en donde el WAF mitigó un total de 1.02 millones, 1.22M de peticiones no llegaron al servidor web ya que fueron atendidas por Cloudflare y por último 3.48k de peticiones desde el servidor.



En la imagen anterior se muestra que se logró generar un total de 105.07 GB de tráfico de datos para el sitio de publicación de resultados del PREP del estado de Puebla. El sitio respondió las peticiones de forma adecuada en todo momento.

El sitio del portal del Instituto Electoral del Estado de Puebla: https://www.ieepuebla.org.mx soportó correctamente el Ataque de Denegación de Servicio con las estadísticas que a continuación se describen.

En la imagen anterior se muestra un resumen del reporte generado del WAF del sitio principal del IEE Puebla el cual muestra que tuvo un total de 5.09k de visitas, 298.04k de peticiones totales, un 28.9% de peticiones atendidas por el cache de Cloudflare.



La anterior imagen muestra un resumen del ancho de banda que se generó durante las pruebas del ataque DoS dando como resultado un total de 52.65GB de tráfico generado, con un pico máximo de 9.36 GB, 15.21GB de ancho de banda en cache.

Conclusión de las pruebas DoS.

Al termino de las pruebas para ambos objetivos https://puebla-extra-sitio-2025.sistemaprep.com y https://www.ieepuebla.org.mx, se concluye que los sitios cuentan con los mecanismos adecuados para resistir y mitigar un ataque de tipo denegación de servicio (DoS). Ambos sitios emplean una solución robusta contra estos ataques mediante el uso de Cloudflare, garantizando su operación continua y eficiente.

6. DICTAMEN DE LA AUDITORÍA

Como resultado de las pruebas y revisiones a la infraestructura y al desarrollo del sistema del "Programa de Resultados Preliminares" (**PREP**) 2025 del Instituto Electoral del Estado de Puebla (IEE Puebla), manifestamos que:

- Los servidores e infraestructura asociada a los procesos del "PREP" son seguros y confiables. Se identificó un hallazgo de riesgo moderado que, si bien no compromete la operación general del sistema, ha sido documentado para su futura atención como parte de las mejoras continuas.
- El **"PREP"** del Instituto Electoral del Estado de Puebla es robusto, cumple con los requerimientos funcionales del sistema y realiza las funciones para las que fue diseñado.

El sistema **"PREP"** del Instituto Electoral del Estado, está en condiciones adecuadas para operar durante la Jornada Electoral del 23 de marzo de 2025.

M. en C. Marcelo Pérez Medel
Responsable de la auditoría