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 2024 para el Instituto Electoral del Estado de Puebla

Informe Final de la Auditoría al Sistema PREP 2024

Periodo de evaluación:

del 1 de marzo al 30 de mayo de 2024

Bitácora de modificaciones

Historia de versiones

Versión	Fecha	Descripción del cambio	Autor
0.0.1	07/abril/2024	Creación del formato.	Paulett Jaqueline Toledo Varela
0.2.0	09/abril/2024	Estructuración Rubros	Yazmin Yanela Santiago Gutiérrez
0.4.1	22/mayo/2024	Pruebas funcionales de caja negra	Axel Pantoja Romo, Paulett Toledo Varela, Ángel Leopoldo Moreno Olivares, Diego Rocha Zamudio
0.6.0	22/mayo/2024	Análisis de vulnerabilidades a la infraestructura tecnológica	Luis Fernando Lira Guzmán, Rafael Hernández Vega
0.8.0	22/mayo/2024	Pruebas de denegación de servicio	Yazmin Yanela Santiago Gutiérrez
0.9.0	22/mayo/2024	Validación del sistema informático del PREP y de sus bases de datos	Fernando Lira Guzmán
1.0.0	27/mayo/2024	1era Revisión	Edgar Mórales Palafox, Felipe de Jesús Gutiérrez López
1.1.0	28/mayo/2024	2da. Revisión	Jesús Hernández Cabrera
1.2.0	29/mayo/2024	Revisión final	Marcelo Pérez Medel

Contenido

1. OBJETIVO GENERAL

Realizar una auditoría informática al Programa de Resultados Electorales Preliminares (PREP) de las elecciones 2024, 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 01 de marzo al 30 de mayo de 2024.

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 2024; 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 07 de febrero al 15 de marzo de 2024.

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 2024 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 27 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 369 pasos, los cuales resultan en un estatus:

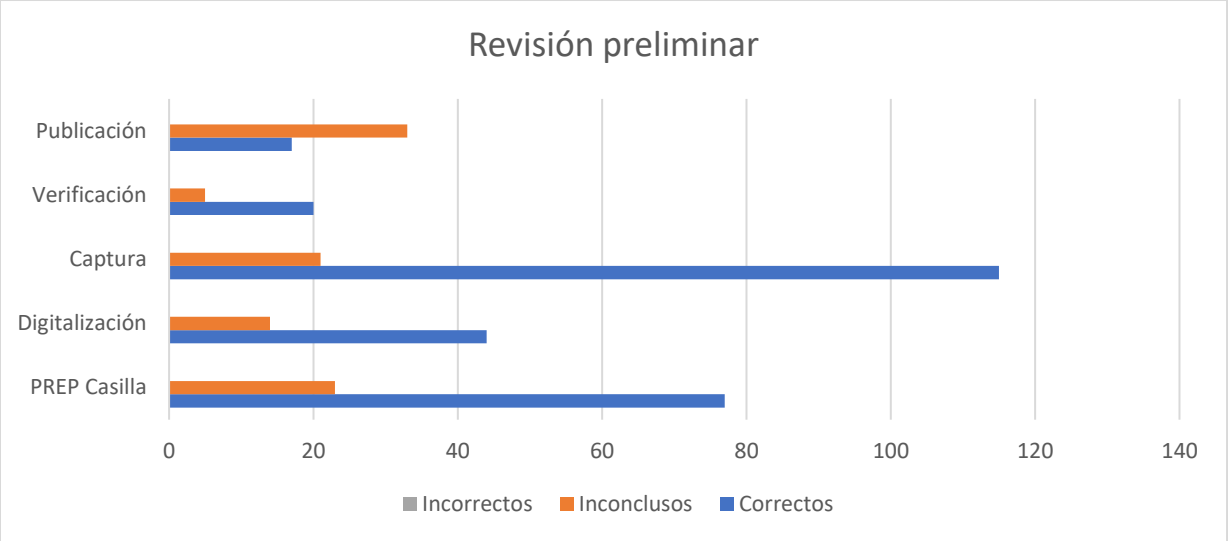
- Correcto. - Al ejecutar el paso, el resultado obtenido es igual al resultado esperado.
- Incorrecto. - Se ejecuta el paso y el resultado obtenido es distinto al esperado.
- Inconcluso. - Se ejecuta el paso, sin embargo, por falta de información en Base de Datos no se puede observar el resultado para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

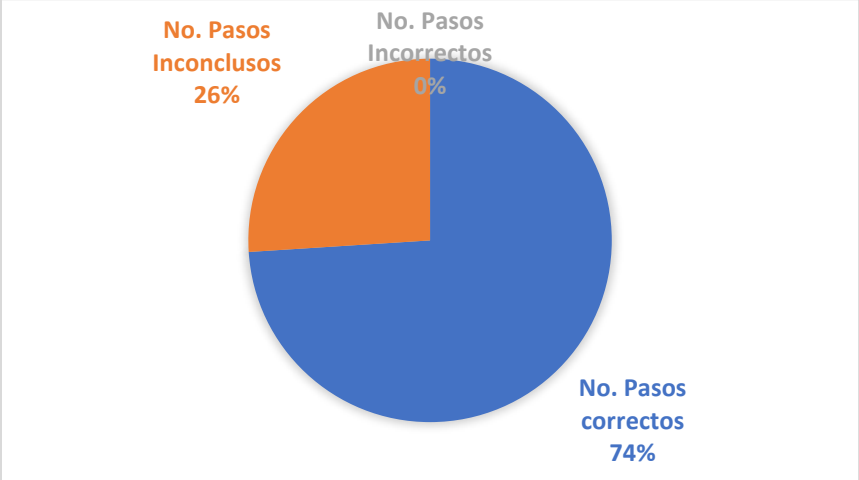
A continuación, se presenta la información obtenida en la ejecución de los casos de prueba para el sistema PREP durante las dos etapas de revisión (Preliminar y final), así como los hallazgos encontrados.

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	77	0	23
Módulo de digitalización	58	44	0	14
Módulo de captura	136	115	0	21
Módulo de verificación	25	20	0	5
Módulo de publicación	50	17	0	33
Total	369	273	0	96

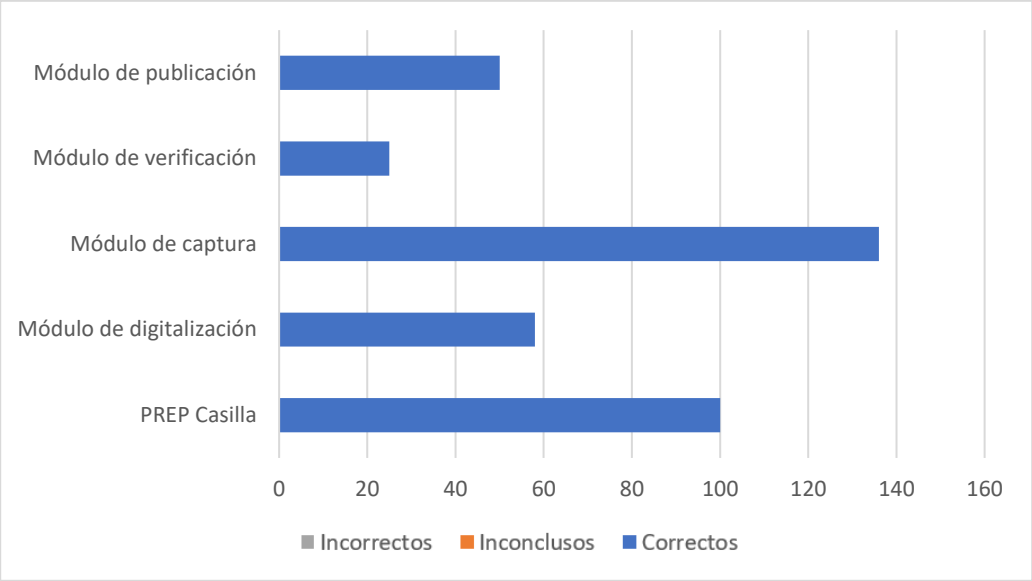


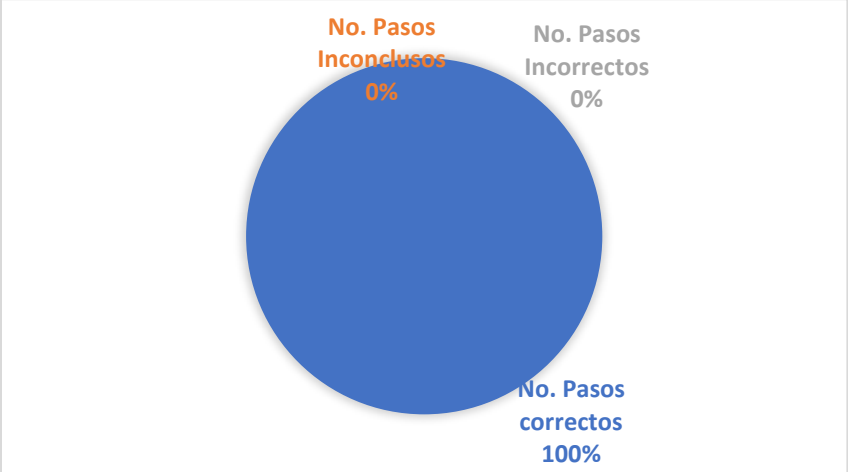


Resultados de la revisión final:

Contrastando con la revisión preliminar, en la siguiente tabla podemos darnos cuenta del aumento en la cantidad de pasos correctos; con 0 pasos incorrectos y 0 pasos inconclusos. Así mismo, podemos notar que tanto el instituto como Grupo PROISI aplicaron algunas de las recomendaciones que se mencionaron en el informe preliminar de las pruebas de caja negra del sistema informático y/o servicios relacionados con tecnologías de la información y comunicaciones para mejorar la funcionalidad del sistema. En cuanto a los hallazgos reportados en el sitio de publicación y la base de datos CSV, se solucionaron y se verificará su correcto funcionamiento durante la ejecución del sistema el día de la jornada electoral.

	Pasos a probar	Correctos	Incorrectos	Inconclusos
PREP Casilla	100	100	0	0
Módulo de digitalización	58	58	0	0
Módulo de captura	136	136	0	0
Módulo de verificación	25	25	0	0
Módulo de publicación	50	50	0	0
Total	369	369	0	0





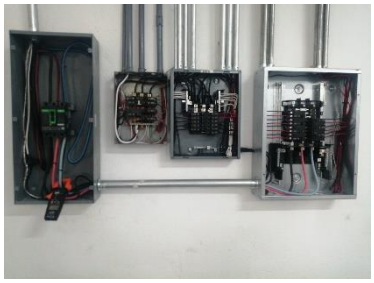
Como parte de las pruebas, se realizó un corte de energía durante el ejercicio de simulacro, en el cual se pudo observar que cuentan con planta de energía que se activa de forma manual y

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 dio a notar la desconexión de manera visible. Todo el CCV continúo con sus operaciones de forma normal.



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

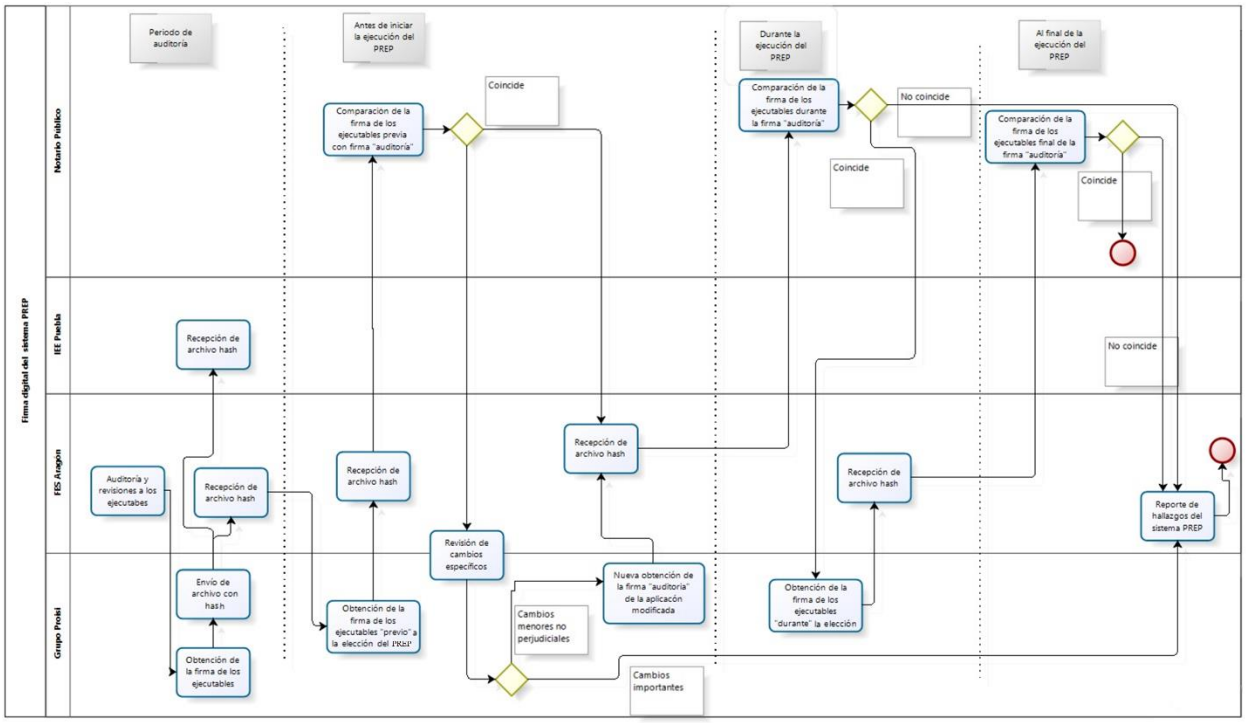
Llevar a cabo un procedimiento técnico para verificar que los programas auditados se encuentren operando desde el inicio y hasta el cierre de operación del sistema informático del PREP, así como que la base de datos se encuentre debidamente inicializada.

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://sitio-prep-puebla-2024.sistemaprep.com, se identificó un solo hallazgo, el uso de una versión desactualizada de una biblioteca. Aunque inicialmente se consideró una vulnerabilidad debido a las posibles exposiciones que podrían presentarse, se realizó una evaluación más profunda y no se encontró evidencia concreta de explotabilidad en el contexto actual del sitio y la protección adicional del Firewall de aplicación Web implementado.

El análisis del sitio relacionado a operaciones del PREP reveló varias vulnerabilidades, aunque las más importantes fueron resueltas, las demás vulnerabilidades permanecen como riesgos aceptados al considerarse de bajo riesgo en el contexto del tipo de información que expone el sistema PREP.

El análisis del sitio https://www.ieepuebla.org.mx reveló varias vulnerabilidades significativas, las cuales fueron reportadas para su atención por parte del Instituto.

Previo a la escritura de este informe, las soluciones a los hallazgos fueron reportados en un documento con capturas de pantalla y verificadas por parte del equipo auditor. Por lo tanto, se dan por cerrados todos los hallazgos relacionados con este activo.

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 tres sitios reportados en los párrafos anteriores implementan está solución como una capa adicional de seguridad.

Revisión de configuraciones

Revisión de la solución tecnológica del sistema PREP.

A partir de la documentación entregada y las sesiones de inspección de consolas vía Zoom, se ha revisado la infraestructura de una plataforma de servicios en la nube. El Grupo PROISI ha desplegado esta solución en un entorno de computación en la nube, destacando los siguientes puntos:

Infraestructura en la Nube

La solución utiliza instancias de computación en la nube optimizadas para procesamientos de alto rendimiento. Estas instancias están configuradas con múltiples unidades de procesamiento virtual, una considerable cantidad de memoria RAM y un amplio almacenamiento en unidades de estado sólido de alta velocidad, facilitando capacidades avanzadas para el procesamiento y análisis de datos.

Sistema Operativo y Servidores Web

Se utiliza un sistema operativo de código abierto reciente, con un software que actúa como servidor web, proxy y suite de seguridad. La configuración de los servidores se ajusta dinámicamente según la demanda.

Gestión de Dispositivos Móviles

Para asegurar la integridad y seguridad de los dispositivos móviles usados en el sistema, se implementan medidas de seguridad específicas, que incluyen cierre de sesión remoto, validación de componentes de hardware de comunicación, almacenamiento seguro de datos, autenticación robusta, y protección de la información de la aplicación.

Servicios de Base de Datos

Se utiliza un servicio de base de datos gestionado, configurado para operar en múltiples zonas geográficas, proporcionando alta disponibilidad y escalabilidad. Esta base de datos como servicio incluye gestión automática, seguridad avanzada y respaldo continuo.

Alta Disponibilidad y Escalabilidad

La arquitectura está diseñada para ser altamente disponible y escalable, incluyendo mecanismos de balanceo de carga y contingencia para asegurar la operación ininterrumpida del sistema.

Acuerdos de nivel de servicio.

Los acuerdos de nivel de servicio con el proveedor de la nube garantizan un alto estándar de disponibilidad y rendimiento, con compensaciones en caso de no cumplir con los términos acordados. Esta arquitectura demuestra un compromiso significativo con la seguridad, robustez y escalabilidad, integrando tecnologías modernas y medidas de seguridad avanzadas para operar el sistema PREP de manera eficiente.

La arquitectura del sistema PREP implementada, exhibe una robustez y seguridad tecnológica de alta calidad, adaptándose eficazmente a las demandas de un sistema crítico. La combinación de soluciones avanzadas de computación en la nube, gestión de bases de datos y dispositivos móviles, junto con una red sólida y redundante, asegura que la plataforma pueda manejar grandes volúmenes de datos con alta disponibilidad y rendimiento, mientras mantiene la integridad y seguridad de los datos electorales. Estos elementos son cruciales para la operatividad y confiabilidad del sistema PREP, garantizando que cumpla con los estándares exigidos para el procesamiento y divulgación eficiente de los resultados electorales. Por lo tanto, la solución propuesta se considera adecuada para satisfacer las necesidades operativas y de seguridad del sistema PREP. Los pocos hallazgos reportados fueron atendidos, pero se recomienda mejorar la calidad de la documentación entregada al auditor.

En el Centro de Captura y Verificación, se llevaron a cabo varias actividades para evaluar y mejorar las configuraciones de la red y la seguridad. Durante la revisión de la estructura de red, se identificaron conexiones de dos proveedores de servicios de Internet, cada uno conectado a un enrutador central de alto rendimiento, lo cual garantiza alta disponibilidad y una gestión eficiente de la red. Las medidas de seguridad implementadas incluyen una mejor gestión de direcciones IP, restricciones de tráfico, defensas contra ataques específicos, y técnicas para mejorar la privacidad y proteger la integridad y disponibilidad del servicio de red.

En las pruebas de seguridad realizadas, se utilizaron portátiles con herramientas especializadas para evaluar la red. Se observó que la red respondía consistentemente a los escaneos de seguridad, indicando robustez en las medidas de protección. No se encontraron puertos abiertos accesibles, reflejando una protección efectiva contra accesos no autorizados. Se hizo la recomendación relacionada con el control de acceso a la red local, la cual fue atendida y reportada.

Finalmente, se revisaron exhaustivamente las estaciones de trabajo para asegurar que no tuvieran acceso a Internet, previniendo así accesos externos no deseados. Las pruebas confirmaron que estas medidas estaban efectivamente implementadas, contribuyendo a la seguridad general del centro.

D) Pruebas de negación 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 2024 y del sitio principal del IEE Puebla, durante el periodo de operación del PREP 2024.

Documentar los hallazgos detectados durante la realización de las pruebas de negación 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 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.

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 1.- Registro de tiempos previos al ataque, orientada a registrar el promedio de los tiempos de respuesta previos al ataque y comparar de forma cuantitativa con las fases posteriores.

Fase 2.- Simulación de tráfico legítimo, esta simulación se realizó empleando herramientas orientadas a probar el comportamiento funcional del sistema.

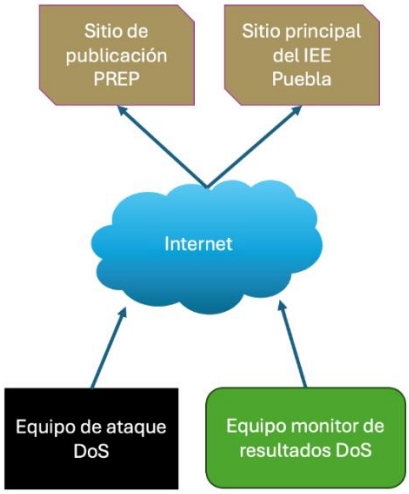
Fase 3.- Etapa de ataque de negación de servicio, en esta fase se emplearon herramientas para realizar un ataque DDoS moderado en ancho de banda y orientado más al ataque lógico a protocolos (TCP, UDP, ICMP y capa de aplicación).

Fase 4.- Pausa, orientada a permitir que el sistema se normalice previo a la etapa 2 del ataque DoS.

Fase 5.- Etapa de ataque de negación de servicio. En esta fase se incluyen las herramientas de la etapa 3 y adicionalmente, Red UNAM para generar un mayor impacto al sistema.

Organización del equipo de seguridad

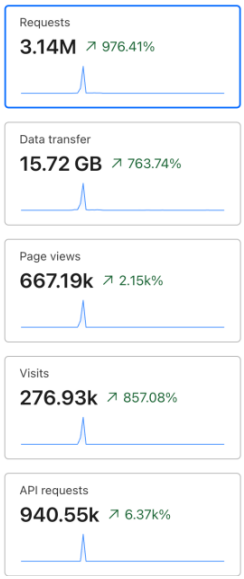
Las pruebas fueron ejecutadas por 12 integrantes del equipo auditor de seguridad, desde 12 puntos diferentes en Internet, 1 de ellos además realizó operaciones de monitoreo y 11 ejecutaron el ataque de forma simultánea.



Resultados

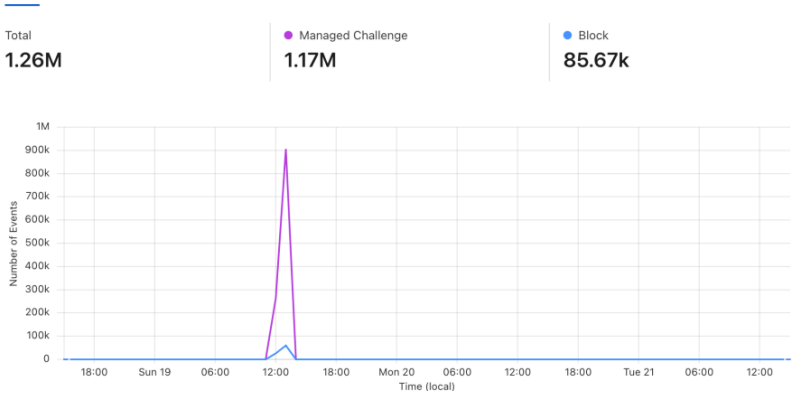
Resultado del sitio PREP Puebla 2024: **https://sitio-prep-puebla-2024.sistemaprep.com/**

En la siguiente imagen se muestra que hubo 3.14M de peticiones, 15.72GB de transferencia de datos, 667.19k en visualizaciones de página, 276.93k visitas y por último 940.55k de solicitudes de API.



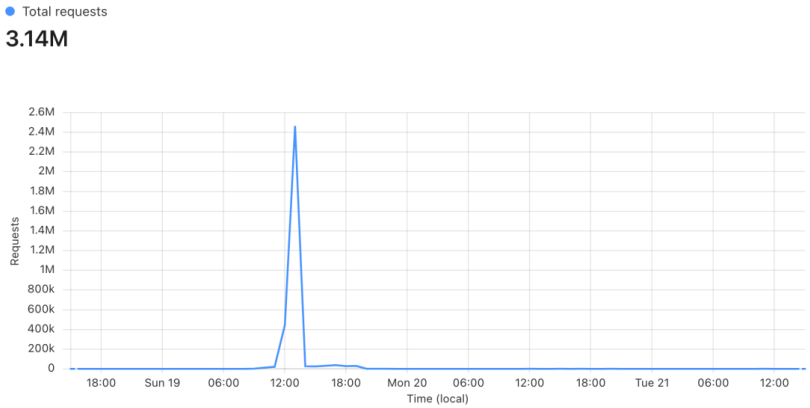
Resumen de estadísticas del reporte proporcionado por el instituto

A continuación, se muestra un resumen del reporte del Firewall en el cual se puede observar que el pico máximo generado fue de 1.26M y un total de 85.67k solicitudes bloqueadas:



Reporte del Firewall.

En la siguiente gráfica se puede observar que se alcanzó un total de 3.14 millones de peticiones HTTP, de las cuales 1.5 millones provenían de México.



Reporte de peticiones de HTTP registradas.

Resultado del sitio principal de IEE Puebla: **https://www.ieepuebla.org.mx**

La prueba de negación de servicio fue realizada el día 22 de mayo del presente año al sitio institucional del IEE Puebla, superando exitosamente el ataque.

Conclusión de las pruebas DoS.

Los sitios del PREP IEE Puebla y el sitio institucional del IEE Puebla superaron las pruebas DoS satisfactoriamente y cuentan con los mecanismos para resistir y mitigar a un ataque de tipo de negación de servicio de forma adecuada y manteniéndose en operación en todo momento.

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**) 2024 del Instituto Electoral del Estado de Puebla (IEE Puebla), manifestamos que:

- Los servidores e infraestructura asociada a los procesos del **"PREP"**, son razonablemente seguros, su nivel de riesgo es muy bajo para la operación del servicio mencionado.
- 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 creado.
- Recomendamos tener especial cuidado con el suministro eléctrico, planta de luz y sistemas de respaldo eléctrico para los equipos de cómputo, esto relacionado con los eventos extraordinarios de corte de energía que han acontecido a nivel nacional en las últimas semanas.

El sistema **"PREP"** del Instituto Electoral del Estado de Puebla, está en condiciones adecuadas para operar durante la Jornada Electoral del 2 de junio de 2024.

M. en C. Felipe de Jesús Gutiérrez López
Responsable de la auditoría