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

Auditoría Informática al Programa de Resultados Preliminares PREP 2024 para el IECM

Informe final de la Auditoría de Software

Periodo de evaluación:
Del 1 de abril al 30 de mayo de 2024

AA

Bitácora de modificaciones

Historia de versiones

Versión	Fecha	Descripción del cambio	Autor
0.0.1	07/abril/2024	Creación del formato.	Marcelo Pérez
0.1.0	09/abril/2024	Estructuración Rubros	Ángel Moreno
0.1.1	02/mayo/2024	Metodología	Ángel Blas de Jesús
0.2.1	22/mayo/2024	Pruebas funcionales de caja negra	Axel Pantoja, Diego Rocha, Ángel Blas de Jesús, Fernando Lira
0.3.0	22/mayo/2024	Análisis de vulnerabilidades a la infraestructura tecnológica	Fernando Lira, Rafael Hernández
0.4.0	22/mayo/2024	Pruebas de negación de servicio	Jesús Hernández, Rafael Hernández
0.5.0	22/mayo/2024	Validación del sistema informático del PREP y de sus bases de datos	Ángel Moreno, Jesús Hernández
1.0.0	28/mayo/2024	1era Revisión	Edgar Morales
1.0.1	29/mayo/2024	2da Revisión	Jesús Hernández
1.0.2	30/mayo/2024	Revisión final	Marcelo Pérez

Contenido

1. OBJETIVO GENERAL

Realizar una auditoría informática al Programa de Resultados Electorales Preliminares (PREP) 2024, del Instituto Electoral de la Ciudad de México 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, mediante un análisis detallado del código, que los aplicativos PREP realizan las funciones descritas en el manual de usuario y solamente esas, es decir, el programa solamente 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.
   - Cumplimiento en buenas prácticas de codificación basado en estándares en donde se protejan los componentes por medio de encapsulamiento, niveles de acceso y buena implementación de estructuras de control.
   - Manejo de errores.
   - Evaluación de desempeño y ausencia de leaks de memoria y 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 (DoS) para comprobar la robustez y disponibilidad del servicio.

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 1 de abril al 31 de mayo de 2024.

B. La auditoría consiste en dos partes: La primera, corresponde a revisión de la funcionalidad e inspección de código fuente; la segunda, identifica posibles vulnerabilidades que tenga el sistema.
C. Se realizó 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. La auditoría se realizó con base a los requerimientos establecidos en el anexo técnico del convenio de colaboración UNAM – IECM 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 las realización de las pruebas OSSTM, 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 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 en relación 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 usará 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. Basándonos en lo que se consideran las mejores prácticas de programación haremos sugerencias para buscar que los cambios sean los menos posibles si es que se necesitan.
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 al 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 permita 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 IECM originado a raíz de las pruebas realizadas.

Durante nuestra participación en la auditoría aparte de realizar todas las revisiones y pruebas que se presentan en las siguientes secciones, visitamos distritos electorales para realizar revisiones y tuvimos presencia en el Instituto durante todos los simulacros y monitoreamos estos desde fuera.

Los resultados se presentan 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 considera lo descrito en el Anexo 13 de 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 1 de abril al 30 de mayo 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 uso se muestra en la Ilustración 1.

	Proyecto:	Auditoría PREP 2024 IECM	
	Institución:	Universidad Nacional Autónoma de México Facultad de Estudios Superiores Aragón Centro Tecnológico Aragón	
No. Caso de prueba:	06	Nombre:	Búsqueda de paquete.

Diseñado por:	Diego Rocha Zamudio
Probado por:	
Fecha de la prueba:	12/04/2024
Tipo de prueba:	Software.
Precondiciones:	Completar el caso de prueba "Comparación de lista de paquetes en base de datos".
Descripción de la prueba:	Se verificarán los flujos principales del caso de uso para la búsqueda de paquete.

Elemento (s) a ser probado		
1		Correcto funcionamiento de "Búsqueda de paquete"

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

Hardware: IPAD/TABLET(Android).

Software: Aplicación móvil del sistema PREP Acopio 2024.

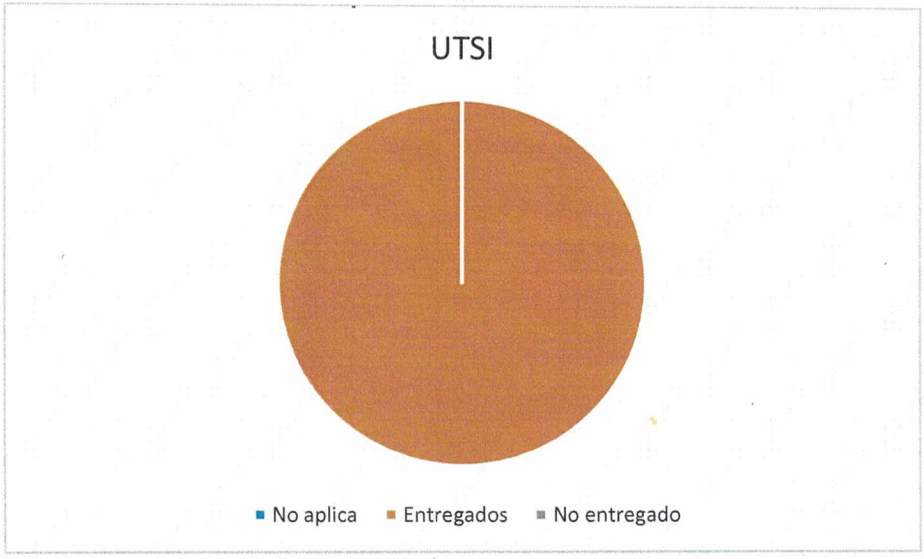
Especificaciones		
Entrada	**Resultado esperado**	**Resultado obtenido**
-Búsqueda del identificador de un paquete en el aplicativo.	-El sistema muestra el paquete solicitado correctamente	-El sistema mostró correctamente la información del paquete solicitado

Ilustración 1.- 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 entregados
UTSI	25	0	25	0



Las pruebas de funcionalidad se realizaron a través de 31 casos de prueba, en ellos se establece el funcionamiento técnico operativo del sistema PREP. Cada caso de prueba contiene un número total de pasos que, al ser revisados, se estableció un total de 466 pasos, los cuales resultan en un estatus:

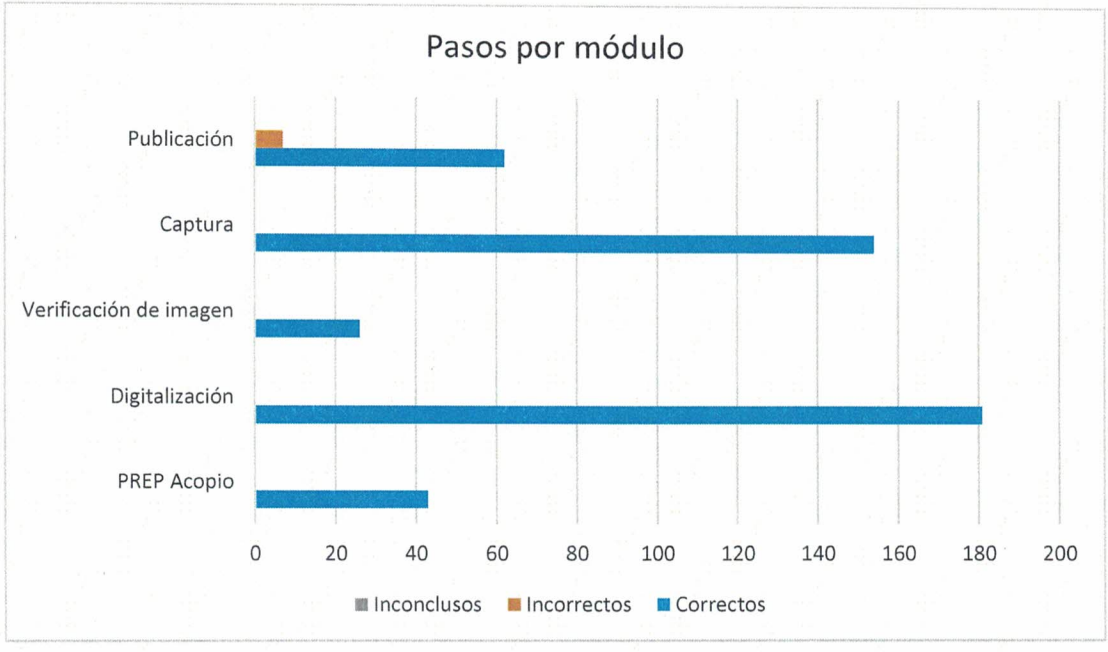
- Correcto. - Al ejecutar el paso, el resultado esperado es igual al resultado obtenido.
- Incorrecto. - Se ejecuta el paso y el resultado obtenido es distinto al esperado.
- Inconcluso. -Se ejecuta el paso, sin embargo, por falta de información en base de datos no se puede observar el resultado para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

Se presenta la información obtenida al ejecutar los casos de prueba para PREP durante las etapas de revisión preliminar y final, posteriormente se presentan los hallazgos encontrados, los solventados y los no solventados.

Resultados de la revisión preliminar:

Al momento de la primera revisión, el flujo de operación estándar funcionaba adecuadamente, pero aún faltaban detalles de la operación de flujos. Adicionalmente, los pasos incorrectos se acordaron revisar en la segunda fase de pruebas.

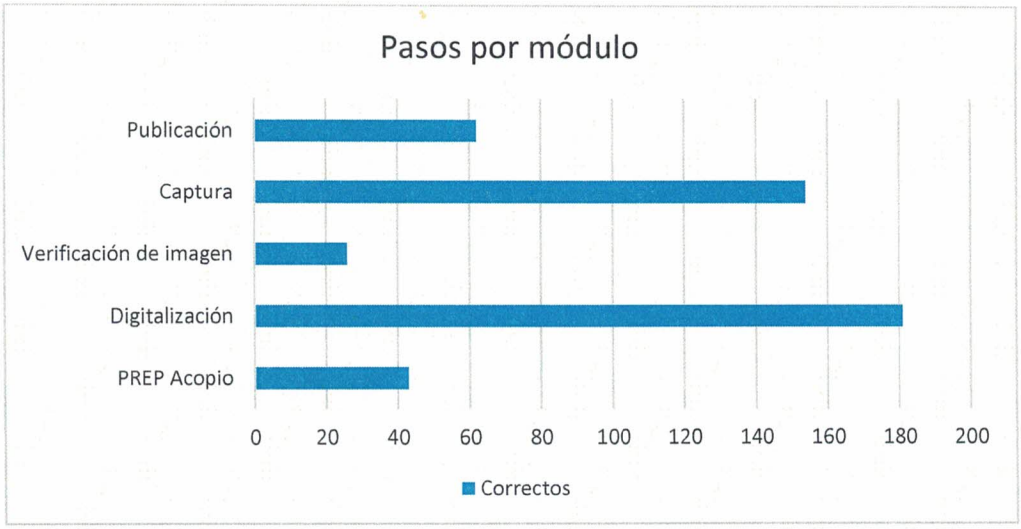
	Pasos a probar	Correctos	Incorrectos	Inconclusos
PREP Acopio	43	43	0	0
Digitalización	181	181	0	0
Verificación de imagen	26	26	0	0
Captura	154	154	0	0
Publicación	62	55	7	0
Total	466	459	7	0



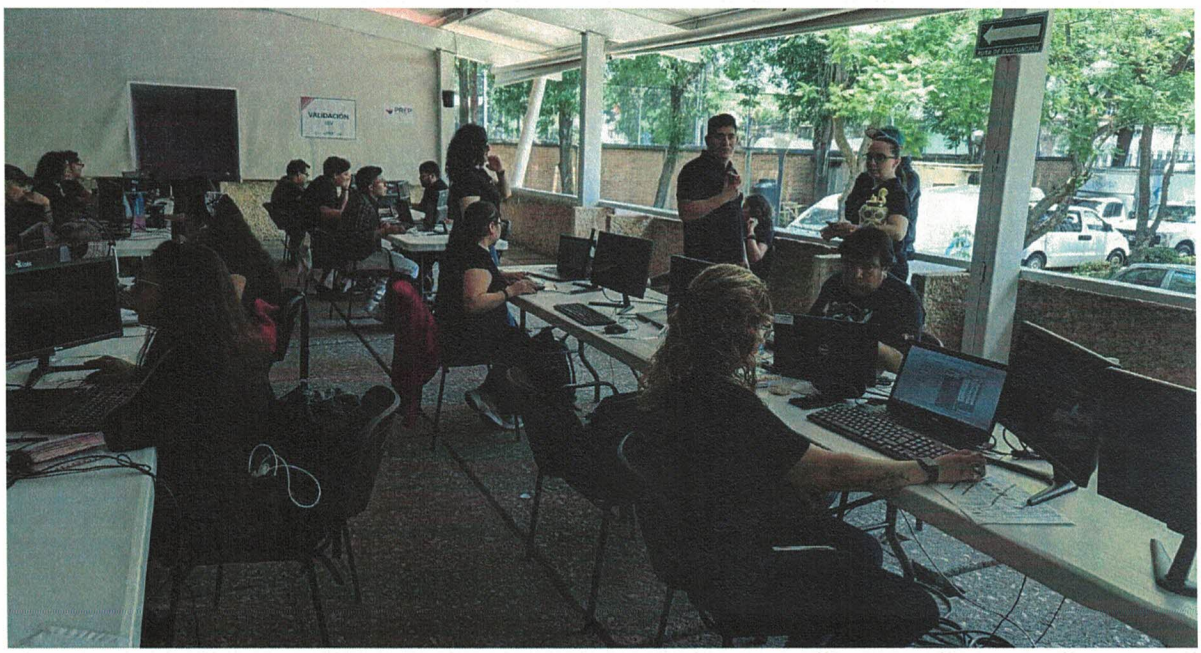
Resultados de la revisión final:

Durante la revisión final se pudo corroborar que todos los hallazgos habían sido subsanados. Referente a los hallazgos reportados en el sitio de publicación y la base de datos CSV, el IECM los remedió durante el segundo simulacro y se verificará su correcto funcionamiento durante la ejecución del sistema el día de la jornada electoral.

	Pasos a probar	Correctos	Incorrectos	Inconclusos
PREP Acopio	43	43	0	0
Digitalización	181	181	0	0
Verificación de imagen	26	26	0	0
Captura	154	154	0	0
Publicación	62	62	0	0
Total	466	466	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, si bien elementos como monitores de apoyo se apagaban, los equipos de cómputo, líneas telefónicas y el servicio de internet permanecían en correcto funcionamiento, permitiendo así continuar con las actividades de captura sin interrupciones. Una vez la planta de energía de respaldo arrancó, los elementos afectados por el corte de luz se encendieron nuevamente.



Adicionalmente, durante las pruebas funcionales se reportaron dos hallazgos de criticidad baja, uno respecto al ciclo de vida y otro al proceso técnico operativo del sistema; mismos a los que la UTSI respondió y a continuación se muestra un resumen:

	Hallazgo
6.1. Ciclo de vida	Para la documentación generada durante las distintas fases del ciclo de vida del sistema PREP, se observa que no hay mucho nivel de detalle.
6.2. Proceso técnico operativo	La distribución en el diseño del aplicativo móvil no es cómoda para el usuario.

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

Objetivo

Validar que el sistema informático del PREP y PREP Casilla que operarán 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 y PREP Casilla, se tendrá que realizar al inicio, durante y al final de su operación.

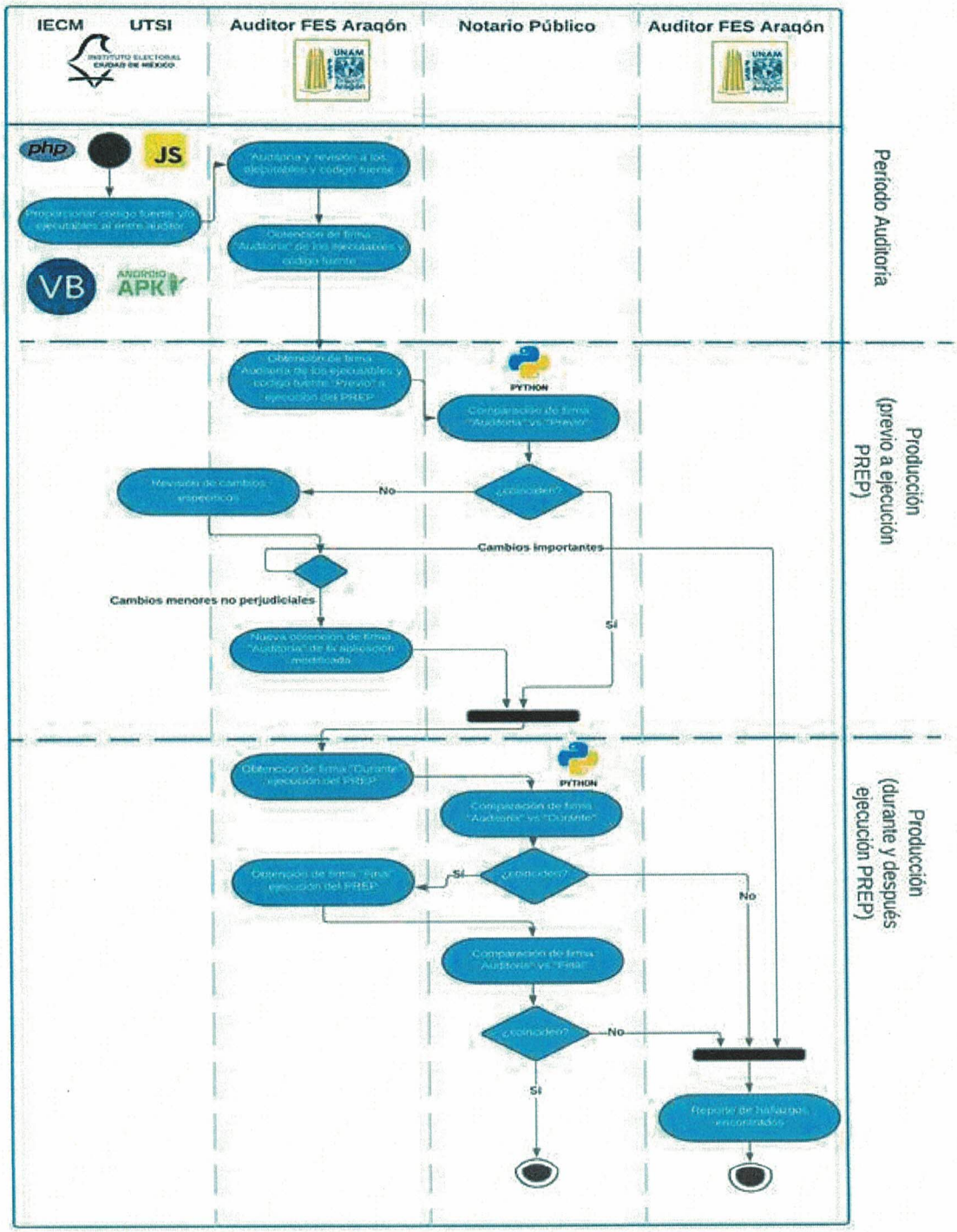
Alcance

- Realizar la firma electrónica del código fuente del PREP 2024.
- Los archivos del PREP 2024 estarán almacenados en el servidor, y la firma de éstos estarán en poder del Auditor externo.

Procedimiento técnico

EL Instituto Electoral de la Ciudad de México en coordinación con la entidad desarrolladora del PREP (la UTSI), harán entrega al ente auditor los archivos con el código fuente, así como los ejecutables que lo requieran, de los cuales se obtendrá una firma por medio de una función SHA-256 (previo al día de ejecución del PREP) una vez compilada la última versión de producción del software.

Diagrama para la firma del sistema PREP



Procedimiento descrito de la firma del sistema PREP

a) Obtención de firma previa a la elección (previo a la ejecución del PREP)

Durante el proceso de auditoría se realizará la firma del sistema PREP mediante la función SHA-256, para posteriormente hacer la comparación al mismo, el día de la jornada electoral. Para el caso de los módulos que requieran de compilación, se verificará que el código fuente coincida con el revisado, se procederá a la compilación y se obtendrá el hash correspondiente del ejecutable.

b) Corroboración de firma el día de la elección (previo a la ejecución del PREP)

El día de la elección, en un acto previo a la ejecución del sistema PREP, se realizará la verificación del software a través de la comparación de la firma obtenida en el punto "a" y la firma generada este día por el ente auditor, la persona con fe pública verificará que las respectivas firmas coincidan.

c) Corroboración de firma el día de la elección (durante la ejecución del PREP)

El día de la elección, mientras el sistema PREP se encuentra en ejecución, se realizará una segunda verificación del software a través de la comparación de la nueva firma, y la firma obtenida en el punto "a", la persona con fe pública verificará que las respectivas firmas coincidan.

d) Corroboración de firma el día de la elección (posterior a la ejecución del PREP)

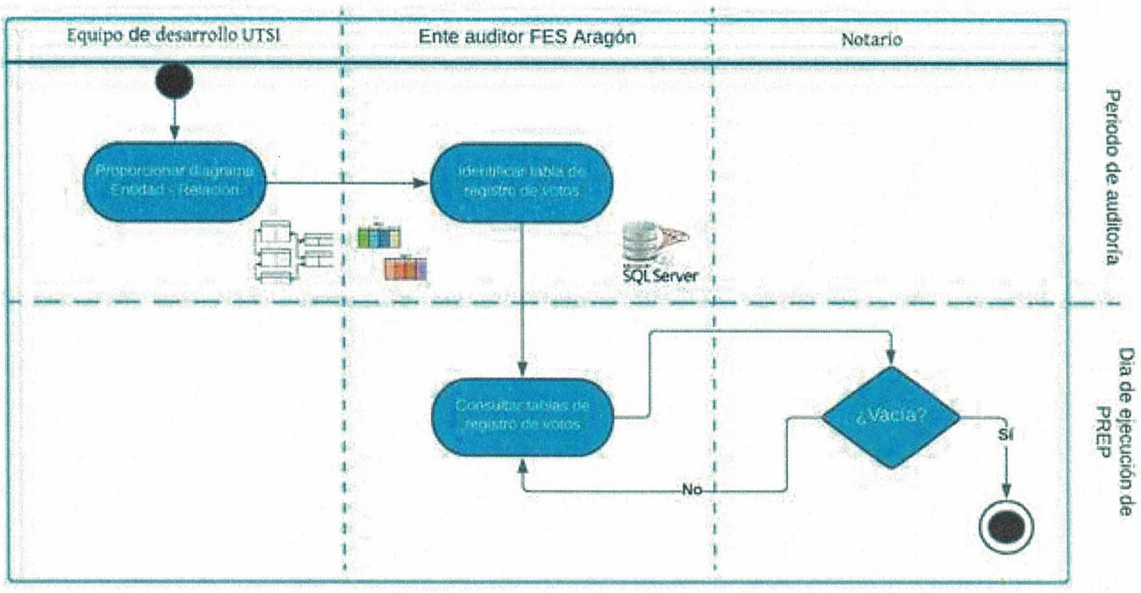
Posterior a la ejecución del sistema PREP, se realizará la verificación del software a través de la comparación de una última firma del mismo, y la firma obtenida en el punto "a", la persona con fe pública verificará que las respectivas firmas coincidan.

Plan

Las actividades, etapas y los responsables de las actividades se pueden apreciar en el diagrama anterior, la firma del código auditado se realizará el día 1 de junio por parte del ente auditor y se generará el código hash, se comprueba que el código es el mismo que el auditado y se instala para su ejecución el día 2 de junio.

El día 2 de junio se verificará que la base de datos se encuentre en cero conforme al procedimiento que se describe en la próxima sección.

Diagrama para la verificación de la Base de Datos PREP



Procedimiento para la verificación de la Base de Datos (debe estar en cero)

a) Identificación de tablas de base de datos
Una vez proporcionada la base de datos y para efectos de auditoría, se comprobará el diseño y se identificarán las tablas que contendrán los registros de votos, con el visto bueno del Instituto Electoral de la Ciudad de México.
b) Verificación de bases de datos en cero

El día de la elección se mostrará ante la persona de fe pública que las tablas mencionadas en el punto "a" se encuentran vacías por medio de una consulta SQL a las mismas.

Roles y responsabilidades

Rol	Responsabilidad
Ente auditor (FES Aragón)	Realizar la generación y comparación de firmas electrónicas del sistema, previo, al inicio, durante y al final de la ejecución del sistema PREP.
Instituto (IECM)	Facilitar y verificar las actividades propuestas en este documento entre las demás entidades.

Entidad desarrolladora (UTSI)	Facilitar al ente auditor acceso al código fuente y/o ejecutables del sistema PREP, además de corregir cambios (solo en caso de existencia).
Persona con fe pública	Dar fe que las firmas SHA-256 generada al terminar de auditar el sistema auditado, sea el mismo SHA-256 generado previo a la ejecución del sistema. Dar fe que las tablas donde se almacenan los registros de votación se encuentren vacías previo a la ejecución del sistema.

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 IECM las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.
- Verificar que las medidas implementadas por el IECM 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 llevarán 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

I. Presentación de hallazgos. El ente auditor deberá presentar un informe preliminar con los hallazgos encontrados, así como la recomendación para atender los mismos.
Para la presentación de hallazgos se utilizará un registro de datos en el que, de forma conjunta el ente auditor y el IECM, puedan dar seguimiento a los mismos.

II. Validación de reporte de hallazgos. El IECM presentará al ente auditor la retroalimentación acerca de los hallazgos encontrados con el fin de descartar falsos positivos (hallazgos que indican incorrectamente sobre la presencia de una vulnerabilidad) y homologar criterios de interpretación de dichos hallazgos.

III. Atención de hallazgos. Una vez validados los hallazgos, el IECM aplicará los diferentes controles necesarios para mitigarlos y atenderlos. Cabe señalar que el ente auditor deberá considerar dentro de su plan de trabajo, otorgar al menos 10 días hábiles para que el IECM pueda atender los hallazgos.

IV. Validación de la atención de los hallazgos. El ente auditor validará que el IECM haya aplicado los controles necesarios para atender a los hallazgos reportados.

Pruebas de penetración (PenTest)

1. Introducción

Las pruebas de penetración consistieron en realizar un descubrimiento de activos en la red, escaneo de vulnerabilidades, análisis de vulnerabilidades y posteriormente seleccionar los activos objetivo. Estas tareas se hicieron de forma manual y empleando la herramienta Nexpose, en conjunto con la herramienta Metasploit Pro, para eventualmente explotar vulnerabilidades viables, resultado del análisis de vulnerabilidades respectivo. Más adelante se presentan los resultados generales.

2. Alcance

Este documento integra la información recuperada durante el proceso de auditoría, e incluye lo siguiente:

- Pruebas de penetración (pentest)
- Revisión de configuraciones de seguridad

Aplicándose los puntos anteriores a elementos de la infraestructura como son, equipos de redes y servidores y las aplicaciones web que en ellos residen, así como las estaciones de trabajo que capturan y envían información.

Se presentarán evidencias que validen los hallazgos obtenidos al realizar las pruebas, de tal forma que el instituto pueda identificar y mitigar (apoyado en las recomendaciones) los riesgos provocados por la existencia de ciertas vulnerabilidades.

3. Clasificación de vulnerabilidades

Como resultado de las actividades descritas anteriormente, se obtendrán ciertos hallazgos provenientes de las pruebas que hayan sido ejecutadas durante el análisis de vulnerabilidades, las pruebas de penetración y la revisión de las configuraciones. Dichos hallazgos deberán ser evaluados con base en un criterio de impactos que se muestra a continuación:

Criterio de impacto a los procesos

Nivel	Impacto	Descripción
1	Moderado	Procesos de baja prioridad se ven afectados, pero no detenidos.
2	Severo	Procesos de alta prioridad se ven afectados, pero no detenidos.
3	Crítico	Procesos de alta prioridad se ven afectados y pueden ser detenidos.

4. Técnicas y vectores de ataque

Durante las pruebas ejecutadas se utilizaron técnicas de descubrimiento y escaneo basadas

en diferentes protocolos y empleando la herramienta Acunetix, para obtener información sobre el sistema que nos permita generar vectores de ataque con altas probabilidades de efectividad.

Entre las técnicas utilizadas se encuentran:

- Escaneos de protocolos basados en modelo TCP/IP de acuerdo con el puerto estándar
- Escaneos de protocolo ICMP
- Trazados de ruta entre IP origen e IP destino
- Escaneos de protocolo ARP
- Pruebas de aislamiento de segmentos de red
- Identificación de servicios y versiones
- Análisis de nivel de parches en el sistema

5. ***Resultado de la verificación de la aplicación de las recomendaciones PenTest.***

En la revisión de una plataforma de difusión PREP, se corrigieron varias vulnerabilidades importantes relacionadas con la seguridad de la información y el cifrado. Sin embargo, se recomienda que mejoren algunos aspectos tales como políticas de seguridad específicas y ajustes en la configuración de los encabezados de seguridad. La atención a estas recomendaciones es importante para proteger adecuadamente la plataforma contra amenazas futuras y asegurar la seguridad de los datos.

La evaluación de una URL relacionada a la infraestructura de desarrollo de aplicaciones, entre ellas PREP, reveló varias oportunidades de mejoras de seguridad, que si bien no son sensibles no deben existir de acuerdo con las buenas prácticas

Durante la revisión de la seguridad en la página web Institucional IECM, se mejoraron varias prácticas, incluyendo aspectos críticos relacionados con la protección de directorios y la encriptación de la comunicación. Adicionalmente a estos avances, se recomienda fortalecer las políticas de seguridad en función de un marco de gestión de información implementando de políticas de seguridad más estrictas. Se recomienda enfáticamente fortalecer estas políticas para asegurar la protección y la integridad de los datos continuamente.
Finalmente, hacemos notar que los tiempos desde el momento en que se pudo revisar el sistema en entorno de producción fueron insuficientes, limitando la efectividad del análisis, por lo que sugerimos que para futuras elecciones se implemente con más tiempo el sistema en un entorno productivo con un margen de tiempo suficiente. Es vital mantener una supervisión y documentación rigurosa para asegurar que las medidas de seguridad sean aplicadas de manera efectiva y continua, contribuyendo así a la resiliencia y seguridad de la infraestructura tecnológica.

Revisión de configuraciones de la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP

1. *Objetivos*

El objetivo es analizar las configuraciones de los activos que conforman la infraestructura tecnológica con base en mejores prácticas de seguridad informática para identificar oportunidades y emitir recomendaciones orientadas al fortalecimiento de ésta.

2. *Alcance*

La auditoría se realiza del 8 de abril al 1 de junio de 2024.
Los alcances de este documento están establecidos en el Anexo 13, del Reglamento de Elecciones de los cuales se consideran:

Capitulo IV, numeral 12 sección II donde se identifican los activos críticos.
Capitulo VII, numeral 15 sección I, II, II, IV donde se determina el espacio físico del CATD y las facilidades con que cuentan sus integrantes

3. *Resultados de la revisión.*

Para la realización de esta primera parte de las revisiones se emiten las siguientes observaciones, diferenciadas entre buenas prácticas y recomendaciones. Estos resultados se basaron principalmente en la documentación proporcionada, incluyendo diagramas de red, escaneos de la red interna y escaneos de vulnerabilidades de los servidores principales. Es importante destacar la ventaja de emplear servicios de computación en la nube en la implementación del sistema de procesamiento de resultados electorales para una organización electoral, ya que ofrece una escalabilidad y flexibilidad significativas, permitiendo una gestión eficiente de los recursos durante períodos de alta demanda electoral, además de proporcionar robustas capacidades de seguridad y cumplimiento que son esenciales para la integridad del proceso electoral.

Segmentación de Red.

En el diagrama de red proporcionado por el IECM, se observa que la segmentación de red está claramente implementada para mejorar la seguridad y el manejo del tráfico dentro de la infraestructura. La infraestructura muestra segmentación de red mediante el uso de subredes específicas para diferentes funciones y tipos de tráfico.

Segmentación funcional de servidores.

Cada servidor dentro de la subred está asignado a una función específica, como se observa con los servidores de bases de datos, servidores de aplicación, y servidores web. Esta segmentación funcional asegura que los servicios relacionados estén agrupados, minimizando el riesgo de interferencias cruzadas y simplificando las políticas de seguridad.

Los servicios de almacenamiento y gestión de datos local están alojados en hosts de virtualización específicos, con un segmento de red aparentemente virtualizado, lo que indica una separación física y lógica del resto de la infraestructura. Esto es importante para la protección de datos y la optimización del rendimiento.

Dispositivos de Red.

Se observó la utilización de dispositivos de seguridad perimetral, como firewalls y gateways de red privada virtual (VPN), para proteger los accesos externos a la red. Se observan dispositivos de seguridad perimetral, como por ejemplo firewalls de alta disponibilidad entre los elementos locales y la computación en la nube y juega un papel crucial en la protección perimetral de la red. Estos firewalls son conocidos por su robusta seguridad y gestión de políticas, lo que permite controlar detalladamente el tráfico que entra y sale de la red.

Conexión segura entre redes locales y la computación en la nube.

La infraestructura desplegada en el diagrama incluye un componente importante para la seguridad y conectividad, que es el gateway VPN, el cual proporciona un puente seguro entre la red local y la nube, permitiendo así la transmisión segura de datos entre estos dos entornos. El ancho de banda configurado en el gateway VPN es suficiente para soportar la carga de tráfico de datos generada por las operaciones sin incurrir en cuellos de botella que podrían afectar el rendimiento de las operaciones.

Revisión de los Certificados Digitales y Configuraciones de Seguridad de Aplicaciones Web.

Como parte de las revisiones de las configuraciones, se realizó la revisión de la validez de los certificados de seguridad para los sitios relacionados con el PREP. Los certificados fueron emitidos por una autoridad certificadora específica y tiene una vigencia durante el periodo electoral. Son escenciales para asegurar la comunicación cifrada y la integridad de los datos transmitidos entre los usuarios y el servidor.

Configuraciones de alta disponibilidad y seguridad para las conexiones desde el exterior(Internet).

En el diagrama proporcionado, se observa el uso de un sistema de seguridad web como punto de entrada para conexiones desde el exterior, el cual se enlaza a un balanceador de carga, esta configuración juega un papel clave en la gestión del tráfico de red y en la mejora de la seguridad y la disponibilidad de los servicios alojados en los activos que ofrecen servicio al exterior.

El sistema de seguridad web actúa como una solución de seguridad que ofrece protección contra ataques de denegación de servicio distribuido (DDoS), ataques de fuerza bruta y otras amenazas de seguridad web. Al ser el punto de entrada desde el exterior, filtra el tráfico malicioso antes de que llegue a los servidores internos, lo que reduce el riesgo de compromiso de la infraestructura.

El sistema también incluye funcionalidades de firewall de aplicación web que ayudan a proteger las aplicaciones web contra vulnerabilidades comunes de seguridad, como

inyecciones SQL y ataques XSS, garantizando que sólo se permita el acceso legítimo.

Revisión de la computación en la nube.

Nos fue proporcionada la documentación técnica derivada de un reporte de revisión de la arquitectura, con el objetivo de identificar riesgos y áreas de mejora. El equipo auditor pone especial énfasis en los aspectos relacionados con la recuperación de desastres. A continuación, se describen los hallazgos y recomendaciones.

Los expertos reportaron que algunas aplicaciones web estaban operando en una única instancia de máquina virtual. Se sugiere que para futuras elecciones valoren la posibilidad de ejecutar las aplicaciones en máquinas virtuales independientes o en su caso prever mecanismos de actuación ante contingencias.

Además, se recomendó utilizar una solución de respaldo en la nube para las máquinas virtuales críticas, proporcionando así una línea de defensa esencial ante cualquier falla imprevista. Esta herramienta facilita la restauración rápida de los sistemas a un estado operativo anterior, minimizando los tiempos de inactividad y la pérdida de datos.

Por último, se sugirió incrementar la alta disponibilidad del sistema implementando redundancia en múltiples zonas de disponibilidad. Esto ayudaría a mitigar los efectos de eventos naturales adversos o interrupciones en servicios secundarios.

Se solicitó al IECM que nos proporcionará información relacionada con las acciones que se tomarían en respuesta a las recomendaciones. Es importante mencionar que para esta fase de la auditoría se recibió escasa información, lo cual limitó la capacidad de realizar una evaluación exhaustiva.

4. ***Conclusiones de la revisión de las configuraciones***

La observación de la infraestructura muestra una buena combinación de tecnologías y estrategias de segmentación de red que resultan en una robusta seguridad y eficiencia operacional. La asignación cuidadosa de funciones específicas a servidores y servicios dentro de subredes dedicadas, evidencia una planificación y ejecución que no sólo protege contra riesgos de seguridad, sino que también optimiza el rendimiento del sistema. Esta integración efectiva de tecnologías refleja un enfoque proactivo en la gestión de la infraestructura de red, asegurando así la integridad y la alta disponibilidad de los servicios críticos.

Durante la revisión de las configuraciones de la infraestructura tecnológica del PREP, se identificaron y abordaron 4 recomendaciones. La implementación de Backup para máquinas virtuales críticas y la alta disponibilidad con redundancia en múltiples zonas se han iniciado, verificaremos su conclusión, previo al inicio de la jornada electoral. La deshabilitación de la funcionalidad de estado del servidor y la modificación de la página raíz fueron completamente resueltas, eliminando riesgos de seguridad asociados. Para futuros ejercicios, sería

beneficioso fortalecer aún más la colaboración con el equipo auditor.

D) Pruebas de negación de servicios.

Objetivo

Realizar ataques de negación 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 IECM, 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, hacia los servicios web que se publican dentro del dominio del IECM, ya sea en su propia infraestructura o en la que provea un tercero.
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.

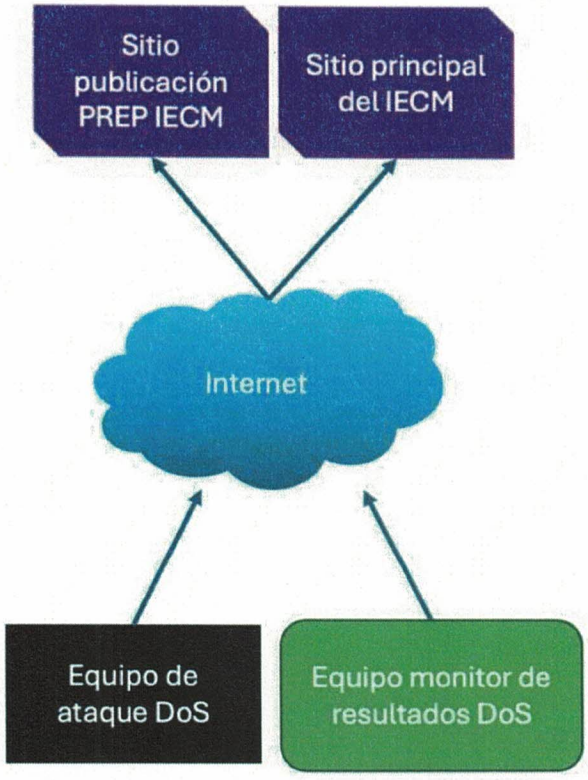
Fase 3.- Etapa de ataque de negación de servicio, en esta fase se emplearon herramientas para realizar un ataque DDoS moderado en ancho de banda y orientado más al ataque lógico a protocolos (TCP, UDP, ICMP y capa de aplicación).

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 los 12 ejecutaron el ataque de forma simultánea.



Organización de la prueba.

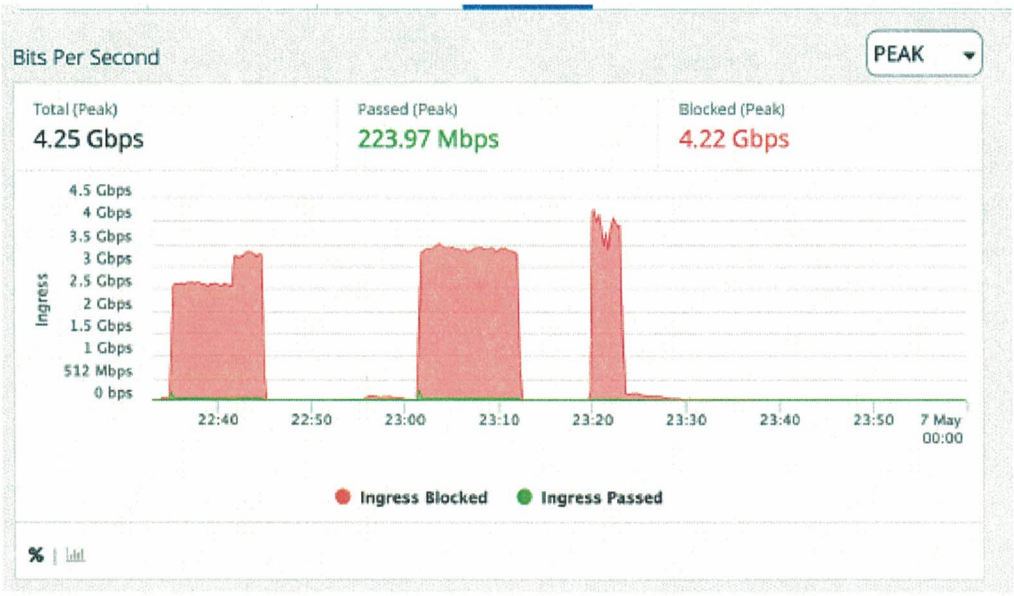
Resultados

Objetivo 1.- https://prep2024.iecm.mx/prep2024

Objetivo 2.- www.iecm.mx

Objetivo 3.- https://actasprep2024.iecm.mx/

Objetivo 4.- https://prepwspriv2024.iecm.mx/



Bits por segundo. Se alcanzó un pico de 4.25 Gbps.

En la anterior gráfica se pueden observar 3 picos, el primero fue el correspondiente al ataque DoS al sitio de publicación PREP por 21 minutos, el segundo al sitio de la página institucional del IECM también por 21 minutos y el tercer pico corresponden a los activos PREP casilla y repositorio de actas (objetivo 4).

Los objetivos 1, 2 y 4 se mostraron erráticas pero funcionales en la primera prueba, se recomendó mejorar la configuración, la cual se realizó en una sesión conjunta, en la segunda prueba los tiempos de respuesta mejoraron considerablemente, por lo que se considera una prueba completamente exitosa.

E) Revisión del Código fuente del sistema PREP.

Introducción

Este informe contiene los resultados de la revisión del código fuente de los sistemas del PREP, del sistema de captura y validación de actas así como de la página web de visualización de las fotografías de las actas por capturar o validar.
La revisión del código del sistema de captura y validación se llevó a cabo manualmente analizando los archivos contenidos en éste. En cuanto al sitio web de las imágenes, su código fue revisado tanto manualmente como utilizando una herramienta que realiza el análisis de manera automática:

SonarQube:
SonarQube es una herramienta de análisis de código que permite identificar errores y vulnerabilidades en proyectos de diferentes lenguajes de programación.

Objetivo general

Revisar el código fuente de los sistemas del Programa de Resultados Electorales Preliminares 2024 (PREP) del Instituto Electoral de la Ciudad de México, para verificar que no existan vicios ocultos en éste. De este modo se puede verificar que no existan errores que puedan provocar un funcionamiento no deseado de los sistemas ni que existan vulnerabilidades de seguridad.

Revisión del código fuente

Métricas de calidad

Deuda Técnica: Es el tiempo que se tendría que invertir para corregir una carencia, ya sea porque es un mal código o porque es una deuda técnica asumida previamente.

Puntuación	Descripción
A	Deuda Técnica menor al 10%. Se considera un proyecto estable y no requiere modificaciones.
B	Deuda Técnica entre el 10% y el 20%. Se considera que está en unos parámetros aceptables, pero es recomendable realizar un chequeo periódico para vigilar que no empeore.
C	Deuda Técnica entre el 21% y el 50%. Valores en los que el proyecto requiere algunas modificaciones. Es necesario revisar si estos errores obtenidos son falsos positivos y que estos no afecten el funcionamiento del sistema.
D	Deuda Técnica entre el 51% y el 100%. Es necesario que se tomen medidas correctivas para hacer más fiable el sistema. Se recomienda revisar si estos errores obtenidos son falsos positivos y que estos no afecten el funcionamiento.
	Deuda Técnica" superior al 100%. Se requieren correcciones mayores

E	tanto de seguridad como de buenas prácticas en la programación. Es necesario revisar si estos errores obtenidos son falsos positivos y que estos no afecten el funcionamiento del sistema.

Evidencias: Número de "malas prácticas" (violaciones) en el código. Por ejemplo, números mágicos, llamar a un método que no es un constructor con el mismo nombre que una clase etc.

Bloqueante	Errores con una alta probabilidad de impactar en el comportamiento de las aplicaciones en producción: pérdida de memoria, conexión a BD no cerrada.
Crítica	Errores con una baja probabilidad de impacto en el comportamiento del sistema o un tema que representa un fallo de seguridad: bloque catch vacío, inyección SQL, etc. El código debe ser revisado.
Mayor	Defecto de calidad que puede tener un alto impacto en la productividad de los desarrolladores: trozo de código no cubierto, bloques duplicados, parámetros no utilizados.
Menor	Defecto de calidad con un leve impacto en la productividad de los desarrolladores: líneas que no deberían ser tan largas, las sentencias "switch" deben tener al menos tres casos.
Info	Ni un error, ni un defecto de calidad, sólo un hallazgo.

Resultados de la revisión de código

Observaciones:
Se encontraron algunos bugs en el código, sin embargo, fueron falsos positivos ya que se encuentran en librerías de terceros.

Con respecto a las vulnerabilidades, se encontró una, sin embargo, también fue un falso positivo porque se encuentra en librerías de terceros.
Sobre los code smells se encontraron algunos detalles sobre convenciones de programación que no se siguieron, de este modo, no afectan al funcionamiento del sistema, pero se recomienda que en versiones posteriores se sigan las convenciones para que el mantenimiento del software sea más sencillo.

El código del sistema de captura y validación PREP 2024 fue revisado manualmente en busca de posibles bugs y vulnerabilidades de seguridad, no se encontraron hallazgos que impacten en la seguridad o el funcionamiento.

F) Verificación a la infraestructura de cómputo y de comunicaciones.

Objetivo

Revisar tanto la infraestructura de cómputo como la de comunicaciones del Instituto para comprobar que son adecuados para la ejecución del sistema PREP 2024.

Respecto a la energía eléctrica se realizaron las siguientes verificaciones:

Criterios a evaluar	Cumple	Observación
Cuentan con planta de energía	Si	Una planta para el Site y otras para el Instituto en general
Tiempo de funcionamiento necesario de la planta desde su activación	Si	75 horas de duración
La planta cuenta con tierra física	Si	
Se cuenta con fusibles de repuesto	Si	
El Site cuenta con UPS	Si	80 Kv (aproximadamente una hora de respaldo), son dos y están en redundancia
Documentos probatorios presentados		Protocolo para situación de emergencia, mantenimiento cada tres meses y compra de fusibles

También se corroboró que:

- El Instituto cuenta con dos proveedores de Internet.
- Cuenta con sistemas redundantes de comunicaciones.
- Sus equipos principales cuentan con doble fuente de poder.
- El Instituto posee su Site en instalaciones propias.
- Cuentan con sistemas de alta disponibilidad.

En general se pudo comprobar que las instalaciones de cómputo y comunicaciones son adecuadas para soportar la ejecución del sistema PREP 2024.

G) Verificación a la infraestructura de cómputo y de comunicaciones de los difusores.

Introducción

Dentro de los requerimientos que se les solicitó a los interesados en participar como difusores de PREP, fue la autorización para que, la Facultad de Estudios Aragón de la Universidad Nacional Autónoma de México, en su calidad de Ente Auditor del sistema PREP 2024 del Instituto Electoral de la Ciudad de México, realizará pruebas lógicas y volumétricas de carga a la infraestructura utilizada para la difusión del PREP 2024.

Objetivo

El propósito principal de esta revisión es confirmar que los publicadores cumplan con los requisitos establecidos por el Instituto Electoral de la Ciudad de México, para asegurar una operación sin contratiempos durante la ventana de tiempo para la divulgación de los resultados del PREP, manteniendo así la integridad y transparencia del proceso.

Pruebas realizadas

Reconocimiento.

Consiste en la recopilación de información pública y accesible sobre el objetivo, con el fin de identificar posibles vulnerabilidades y puntos de entrada. Esta en una fase inicial de las pruebas de penetración, también conocida como fase de "reconnaissance" o "footprinting," incluye actividades como la enumeración de subdominios, la búsqueda de registros DNS, la identificación de direcciones IP, la recopilación de información WHOIS, y la exploración de metadatos en archivos públicos vía internet.

Escaneo.

La fase de escaneo en un proceso de Pen Test es donde se profundiza en la identificación de vulnerabilidades y configuraciones específicas del sistema objetivo. Durante esta etapa, los evaluadores utilizan herramientas automatizadas para escanear puertos, identificar servicios y versiones de software en ejecución, y detectar posibles puntos débiles.

Pruebas de negación de servicio.

Se realizaron pruebas de negación de servicio como parte de la revisión de seguridad para evaluar la resistencia de los sistemas ante ataques cibernéticos. Estas pruebas incluyeron ataques utilizando protocolos TCP, UDP, ICMP y en la capa de aplicación HTTP. Los ataques simulados fueron del tipo lógico y de gran volumen, como inundaciones SYN y ICMP, amplificación DNS, y el ataque Slowris, ejecutándose de manera concurrente para representar condiciones reales y verificar la capacidad de respuesta de los sistemas involucrados.

6. Dictamen de la auditoría

Como resultado de las pruebas y revisiones a la infraestructura y el desarrollo del sistema del "Programa de Resultados Preliminares" (**PREP**) 2024 del Instituto Electoral de la Ciudad de México, manifestamos que:

- La infraestructura y los servidores asociados a los procesos del **"PREP"** demuestran un nivel adecuado de seguridad para la operación actual, aunque se recomienda prestar particular atención a las medidas de protección durante periodos electorales.
- El **"PREP"** del Instituto Electoral de la Ciudad de México es robusto, confiable, y cumple con los requerimientos funcionales del sistema, realiza el 100% de las funcionalidades para las que fue creado y no realiza ninguna actividad fuera de las que están descritas en la documentación del sistema y no contiene vicios ocultos.
- Se recomienda realizar constantemente el monitoreo de todo el sistema.

El sistema **"PREP"** del Instituto Electoral de la Ciudad de México está en condiciones para operar durante la jornada electoral del 2 de junio de 2024.

ATENTAMENTE

"Por mi raza hablará el espíritu"

Ciudad Nezahualcóyotl Estado de México a 30 de mayo de 2024

M. en C. MARCELO PÉREZ MEDEL

Responsable de la auditoría