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

Auditoría Informática al Programa de Resultados Preliminares PREP 2021 para el IECM

Informe final de la Auditoría de Software

Periodo de evaluación:
Del 7 de abril al 7 de junio de 2021

Bitácora de modificaciones

Historia de versiones

Versión	Fecha	Descripción del cambio	Autor
0.0.1	07/abril/2021	Creación del formato.	Marcelo Pérez Medel
0.1.0	09/abril/2021	Estructuración Rubros	Angel Moreno Olivares
0.1.1	02/mayo/2021	Metodología	Ariadne Ivette Olarte Cetina
0.2.1	24/mayo/2021	Pruebas funcionales de caja negra	Axel Pantoja, Diego Rocha, Paulett Toledo, Angel Blas de Jesús
0.3.0	24/mayo/2021	Análisis de vulnerabilidades a la infraestructura tecnológica	Rodrigo Raygadas Baez, Yazmin Santiago
0.4.0	24/mayo/2021	Pruebas de negación de servicio	Jesús Cabrera, Rafael Hernández Vega
0.5.0	28/mayo/2021	Validación del sistema informático del PREP y de sus bases de datos	Angel Moreno, Jesús Hernández Cabrera
1.0.0	31/junio/2021	1era Revisión	Edgar Morales Palafox
1.0.1	1/junio/2021	2da Revisión	Jesús Hernández Cabrera
1.0.2	2/junio/2021	Revisión final	Marcelo Pérez Medel

1. OBJETIVO GENERAL

Realizar una auditoría informática al Programa de Resultados Electorales Preliminares (PREP) 2021, 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 7 de abril al 7 de junio de 2021.

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 a continuación:

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 2021; de dicho documento se toman en cuenta:

- Título II, Capítulo II, numeral 4.
- Título II, Capítulo III, numeral 8.II, 8.III, 9 y 10.I.

De acuerdo al 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 7 de mayo alal 31 de mayo de 2021.

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:	Auditoria SCR 2018 IECM	
	Institución:	Universidad Nacional Autónoma de México Facultad de Estudios Superiores Aragón Centro Tecnológico Aragón	
No. Caso de prueba:	26	Nombre:	Supervisión de casillas

Diseñado por:	Jesús Hernández Cabrera	
Probado por:		
Fecha de la prueba:		
Tipo de prueba:	Software.	
Precondiciones:	Haber ejecutado el caso de prueba de pantalla de inicio del módulo de supervisión del sistema.	
Descripción de la prueba:	Se verificarán los flujos principales del caso de uso para visualizar la información del módulo de supervisores.	
Elemento (s) a ser probado		
1		Verificación de la información del usuario mostrada en la parte superior de la pantalla.
2		Verificación del funcionamiento del menú superior "Avance en la captura de las casillas de la muestra" y de sus botones.
3		Verificación de cada una de las tablas y gráficos mostrados en las diferentes pantallas.
4		Verificación de los datos mostrados en las gráficas.
Configuración de la prueba (hardware, software, base de datos, tiempo)		
Hardware: Computadora en Distrito validado por el IECM con acceso a la red del sistema SCR. **Software:** Navegador con acceso a la ruta del sistema. **Base de datos:** Se requiere un usuario con privilegios de sólo lectura sobre las tablas de administración		

Especificaciones		
Entrada	**Resultado esperado**	**Resultado obtenido**
-Uso del botón "Mapas":	-Se muestra un mapa de una demarcación territorial (inicial por defecto es Azcapotzalco) dividida por estratos, cada estrato tiene un color según su avance de casillas.	-El mapa se mostró correctamente.

Ilustración 1.- Formato de casos de uso

Basándonos en lo que se consideran las mejores prácticas de programación se realizaron sugerencias buscando que los cambios fueran los menos posibles en caso de ser necesarios.

Criterios utilizados para la auditoría

Los hallazgos encontrados durante la prueba se agregan a una matriz y posteriormente se clasifican de acuerdo con nivel de criticidad que presenten en relación con el impacto que se genere. Los niveles de criticidad que se utilizarán son informativo, baja, media y alta, siendo el primero el de menor importancia y el último el de mayor; por otra parte, el instituto debe atender con prioridad los hallazgos de nivel alto.

Nivel de criticidad	Descripción	Prioridad para ser atendido
Alto	El sistema no cubre con la funcionalidad señalada en los lineamientos, convenio o documentos de análisis.	Alta
Medio	El sistema cubre parcialmente la funcionalidad, el sistema puede operar en capacidad mínima.	Media
Bajo	El sistema cubre con la funcionalidad, sin embargo, se encuentran detalles de diseño, información al usuario, entre otras.	Baja

Resultados

Las pruebas de funcionalidad se realizaron a través de 22 casos de prueba, en ellos se establece el funcionamiento técnico operativo del sistema PREP y PREP Casilla. Cada caso de prueba contiene un número de pasos que a ser revisados, para dichas pruebas se estableció un total de 326 pasos, los cuales resultan en un status:

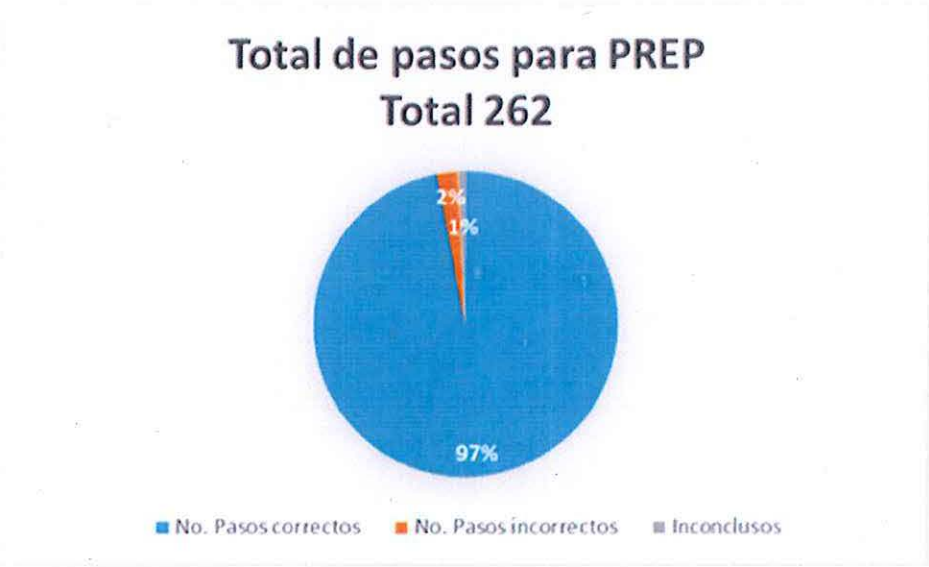
- Correcto. - Al ejecutar el paso, el resultado esperado es igual al resultado obtenido.
- Incorrecto. - Se ejecuta el paso y el resultado obtenido es distinto al esperado.
- Inconcluso. -Se ejecuta el paso, sin embargo, por falta de información en base de datos no se puede observar el resultado para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

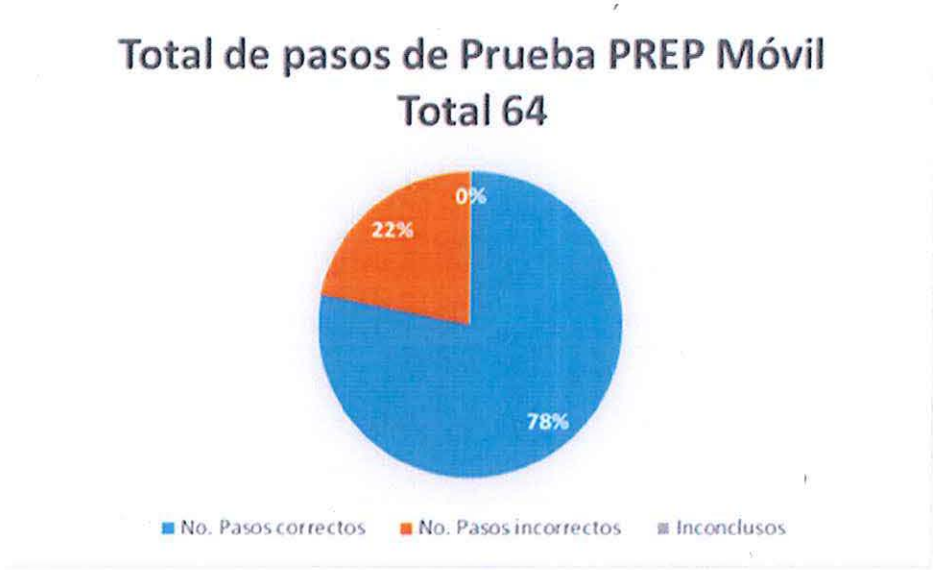
Se presenta la información obtenida al ejecutar los casos de prueba para PREP y PREP Casilla durante las etapas de revisión preliminar y final, posteriormente se presentan los hallazgos encontrados, los solventados y los no solventados.

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 alternos, es decir, cuando la operación trata con excepciones.

	Pasos a probar	Correctos	Incorrectos	Inconclusos
PREP	262	254	6	2
PREP Casilla	64	56	8	0
Total	326	310	14	2

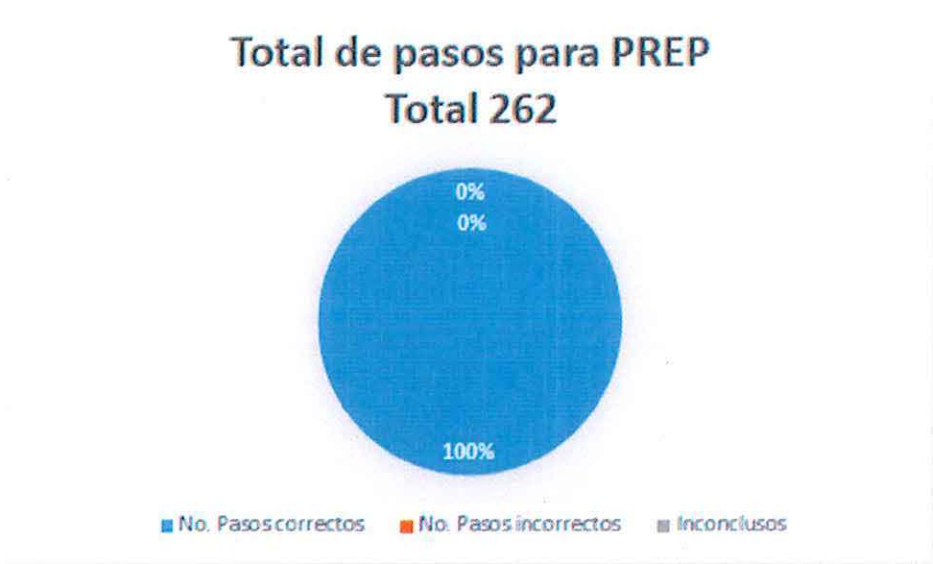


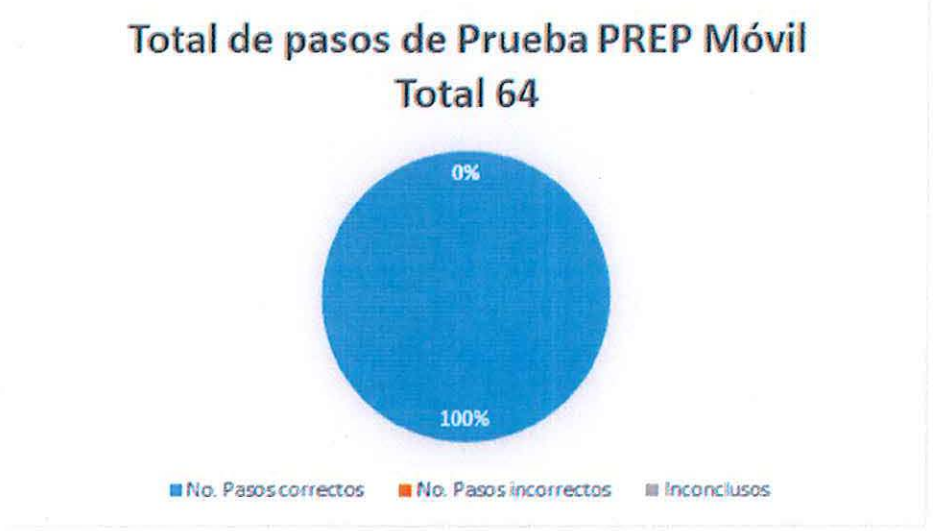


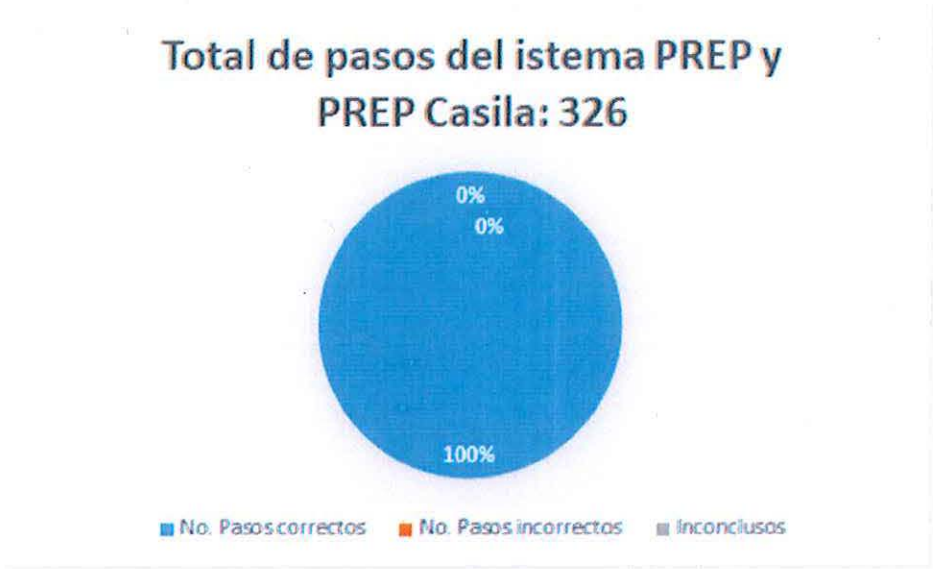
Resultados de la revisión final:

Durante la revisión final se pudo corroborar que todos los hallazgos habían sido subsanados y el manejo de flujos alternos estaba completamente implementado. Para el hallazgo que refiere a dar claridad entre la información que se publica en el portal y la que se obtiene en el csv de descarga de datos, el IECM lo resolvió y se verificará su correcto funcionamiento durante la ejecución del sistema el día de la jornada electoral.

	Pasos a probar	Correctos	Incorrectos	Inconclusos
PREP	262	262	0	0
PREP Casilla	64	64	0	0
Total	326	336	0	0


Total de pasos para PREP
Total 262
0%
0%
100%
No. Pasos correctos
No. Pasos incorrectos
Inconclusos


Total de pasos de Prueba PREP Móvil
Total 64
0%
100%
No. Pasos correctos
No. Pasos incorrectos
Inconclusos



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.

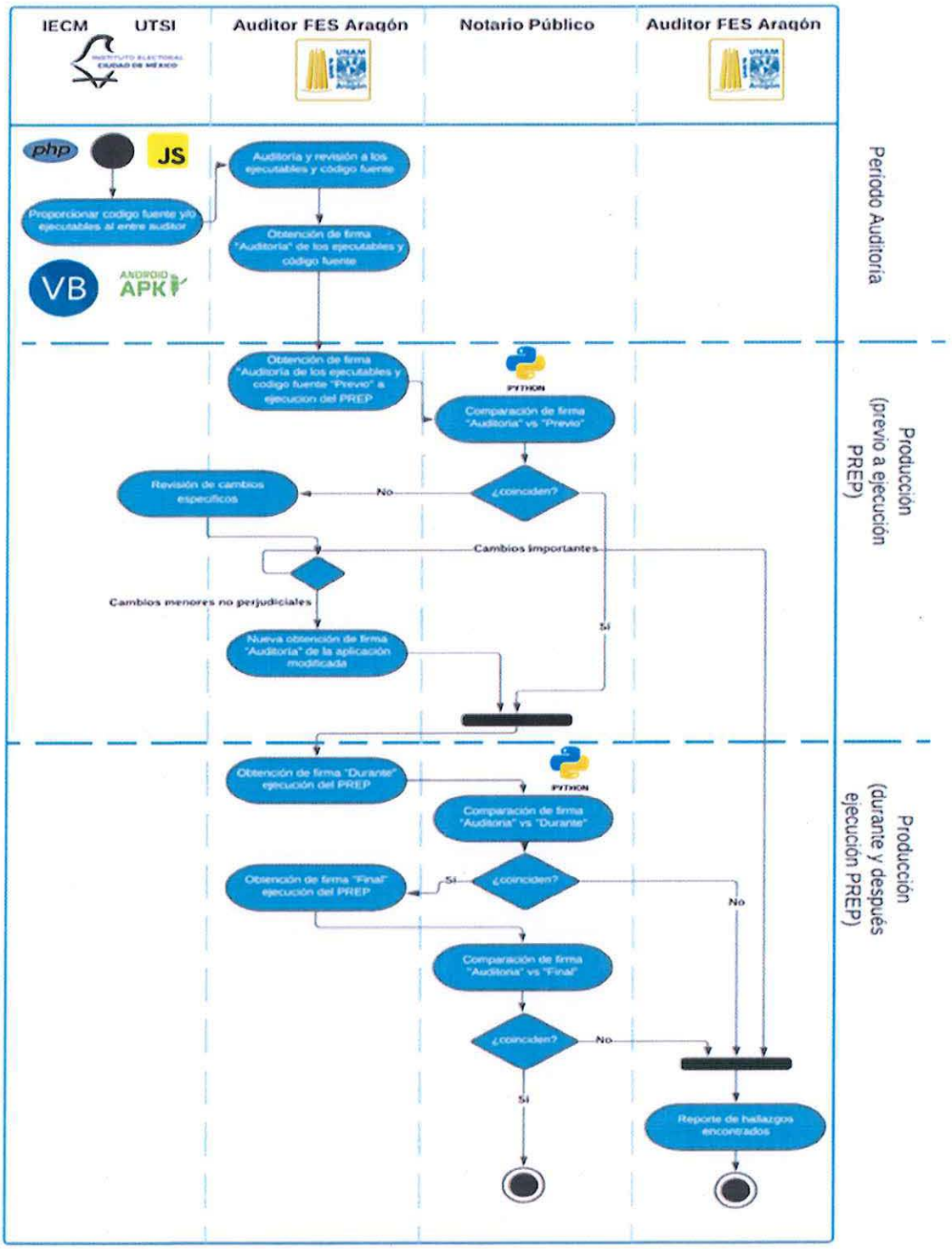
Alcance

- Realizar la firma electrónica del código fuente del PREP 2021.
- Los archivos del PREP 2021 estarán almacenados en el servidor, y la firma de éstos estarán en poder del Auditor externo.
- Los archivos firmados electrónicamente serán grabados en una USB, la cual quedará bajo resguardo del Secretario Ejecutivo.

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)

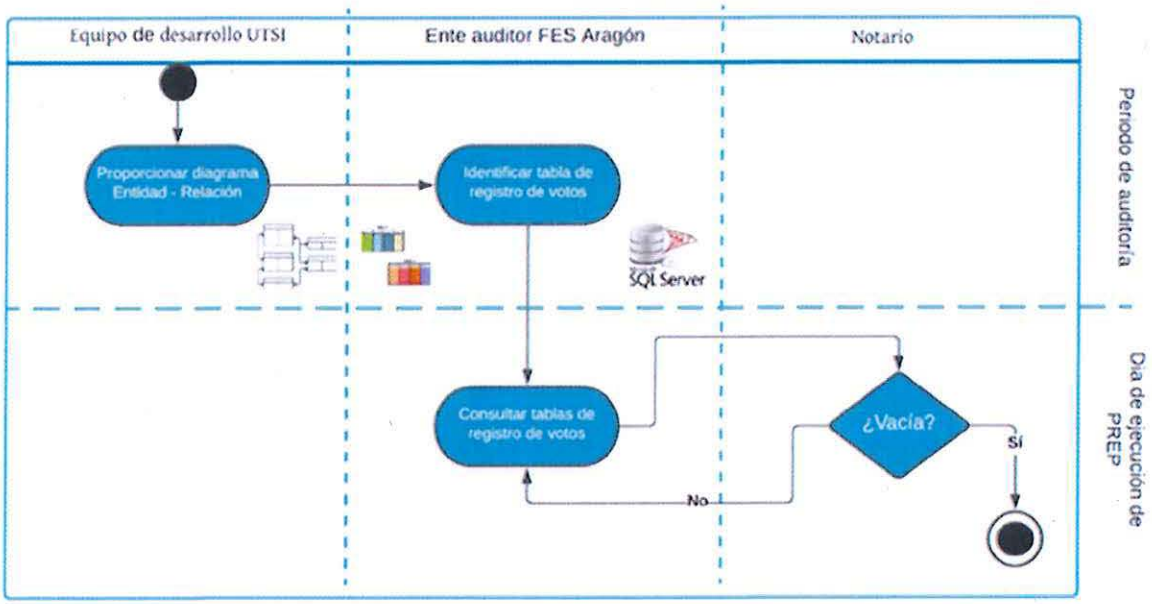
Posterior a la ejecución del sistema PREP, se realizará la verificación del software a través de la comparación de una última firma del mismo, y la firma obtenida en el punto "a", la persona con fe pública verificará que las respectivas firmas coincidan.

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 3 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 6 de junio.

El día 6 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 Nexpose, 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***

De acuerdo al carácter de la fase de pruebas (descubrimiento), se detectaron un total de 1701 hallazgos los cuales fueron reportados en el informe correspondiente al IECM para su revisión y remediación.

El IECM realizó actividades de remediación las cuales fueron informadas, dentro de las cuales sobresale la sustitución del servidor, reinstalando desde cero el sistema operativo y motor de base de datos, aplicando todos los parches de seguridad, migrando las Base de datos y respetando el direccionamiento previo, para no causar impacto en los flujos de comunicación hacia la misma.

Para validar las remediaciones se volvió a ejecutar pruebas de escaneo de vulnerabilidades y en primera instancia se observó que el resultado de la segunda ejecución del escaneo de las vulnerabilidades, redujo el total de hallazgos a 92, los cuales fueron analizados para determinar la superficie de ataque dando como resultado que solo 2 hallazgos son explotables, uno de ellos se resolvió con la

reinstalación del servidor que anteriormente se menciona y el segundo relacionado con un hallazgo de nivel crítico, por lo cual se realizó una reunión con las áreas interesadas del IECM para determinar la mejor opción disponible para remediarlo.

El IECM informó que dicha remediación será aplicada posterior a la entrega de este informe, por lo que será revisada previo a la operación del sistema y será reportada en el informe de evaluación.

Revisión de configuraciones

1. *Objetivos*

El objetivo es analizar las configuraciones de los servidores 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 2021.
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

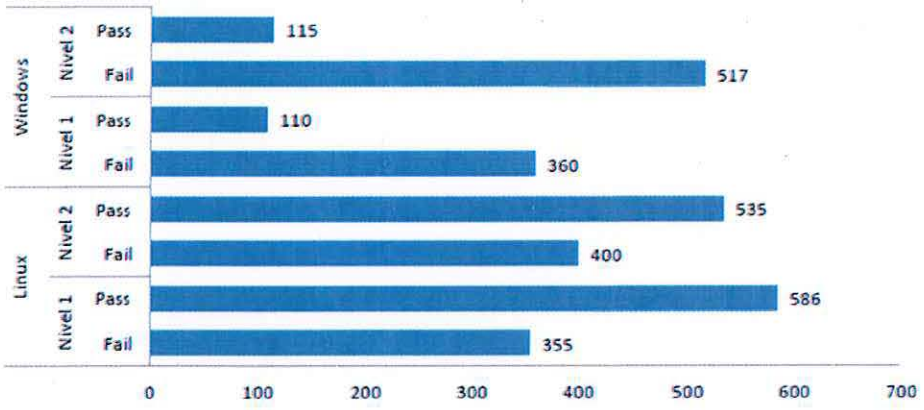
3. *Resultados*

Los análisis de configuraciones se realizaron el 28 mayo del 2021 utilizando las referencias de robustecimiento de seguridad del CIS (Center for Internet Security). Estas referencias cuentan con diferentes niveles de seguridad conocidos como perfiles, a continuación, se definen los perfiles utilizados durante la auditoria.

El perfil de nivel 1 se considera una recomendación básica de seguridad que se puede implementar rápido y está diseñado para no tener un impacto en el rendimiento. La intención de este nivel es reducir la superficie de ataque sin obstaculizar la funcionalidad de los sistemas.

El perfil de nivel 2 está destinado a entornos donde la seguridad es primordial. Las recomendaciones asociadas a este perfil pueden tener un efecto adverso en los sistemas si no se implementan de manera adecuada.

Los resultados obtenidos de las pruebas evaluadas de forma exitosa por sistema operativo son las siguientes:



De acuerdo a los resultados anteriores, se recomendó al Instituto implementar al menos todas las recomendaciones del nivel 1 de acuerdo al CIS tanto para sistemas operativos como para servicios, por ejemplo, bases de datos, servidores web, gestión remota, etc.

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

Una estrategia de seguridad debe tener contemplar al menos dos elementos, el primero, reducir la superficie de ataque y la segunda implementar mecanismos de

detección de intrusos.

La revisión de las configuraciones forma parte de la reducción de superficie de ataque, en este ámbito se encontró que los servidores cuentan con algunas de las recomendaciones de seguridad del CIS para ambos perfiles evaluados, sin embargo, se recomienda mejorar la seguridad de los servidores realizando la configuración de nivel 1.

Al implementar estas recomendaciones, el instituto podrá mejorar la madurez de seguridad en los sistemas electorales y con ello generar una mejor estrategia.

D) Pruebas de negación de servicios.

Objetivo

Realizar ataques de negación de servicio que permitan identificar, evaluar y aplicar las medidas necesarias para asegurar la correcta y continua disponibilidad del servicio Web de los sitios de publicación de resultados del PREP y del sitio principal del IECM, durante el periodo de operación del PREP.

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, en su propia infraestructura y en la que provea un tercero. En este caso se proporcionaron los sitios siguientes:

Objetivo 1.- prep2021.iecm.mx:8010
Objetivo 2.- www.iecm.mx
Objetivo 3.- prepwspriv.iecm.mx:8010

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.
Tráfico de red malintencionado, consistente en paquetes de red malformados.

Las pruebas mencionadas anteriormente deberán realizarse de manera concurrente. Los ataques de negación de servicio deben contemplar, al menos, tráfico de red malintencionado con las siguientes características:

Ataques volumétricos por protocolo TCP
- Al menos de 400 Mbps de throughput
- Al menos realizar SYN FLOOD

Ataques volumétricos por protocolo UDP
- Al menos de 400 Mbps de throughput
- Al menos realizar DNS AMPLIFICATION

Ataques volumétricos por protocolo ICMP
- Al menos de 400 Mbps de throughput
- Al menos realizar ICMP FLOOD

Ataques en la capa de aplicación (HTTP)
- Al menos realizar SLOWRIS ATACK

Las pruebas mencionadas anteriormente deberán realizarse de manera concurrente; considerando la generación de tráfico malintencionado (SYN FLOOD, DNS AMPLIFICATION, ICMP FLOOD, SLOWRIS ATACK) en un volumen que represente las condiciones de un ataque.

Durante las pruebas, cada simulación de ataque deberá apegarse a las condiciones de un ataque para hacer que el sitio web que se esté probando quede fuera de línea (no disponible) por, al menos 2 minutos, previo a que el OPL efectué la contramedida para

la mitigación.

Tipos de ataque

Se realizaron ataque de tipo: SYN FLOOD, DNS AMPLIFICATION, ICMP FLOOD y de CAPA DE APLICACIÓN, los cuales se perpetraron a través de los protocolos TCP, UDP, ICMP y HTTP.

TIPO DE ATAQUE	PROTOCOLO
SYN FLOOD	TCP/IP
DNS AMPLIFICATION	UDP
ICMP FLOOD	ICMP
CAPA DE APLICACIÓN	HTTP

Resultados de las pruebas de negación de servicio.

La ventana de tiempo asignada fue de las 21:00 horas del 30 de abril y hasta las 01:00 horas del primero de mayo en donde la primera hora se empleó para realizar las últimas configuraciones de las herramientas a utilizar. De las 10:05 y hasta las 00:23 horas des siguiente día se ejecutaron pruebas en 5 fases para cada sitio:

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 la herramienta jMeter orientada a probar el comportamiento funcional del sistema.

Durante la fase de preparación se hicieron las adecuaciones para cumplir los requisitos de sesión HTTP configurados en el WAF Imperva, se configuraron la cantidad de hilos para la simulación y la cantidad de hilos a incrementar a través del tiempo.

Fase 3.- Etapa 1 de ataque de negación de servicio, en esta fase se emplearon herramientas para realizar un ataque DoS moderado en ancho de banda y orientado más al ataque lógico a protocolos.

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

Fase 5.- Etapa 2 de ataque de negación de servicio, en esta fase se incluyen las herramientas de la etapa 3 y adicionalmente se agregaron 5 herramientas.

Organización del equipo de seguridad.

Las pruebas fueron ejecutadas por 10 integrantes del equipo auditor de seguridad, desde 10 puntos diferentes en internet y red UNAM (remoto), 2 de ellos realizando operaciones de monitoreo y 8 ejecutando el ataque de forma simultánea.

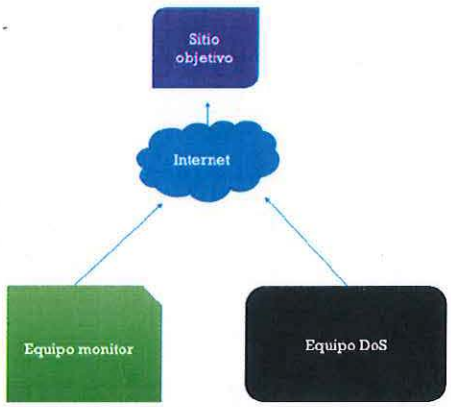
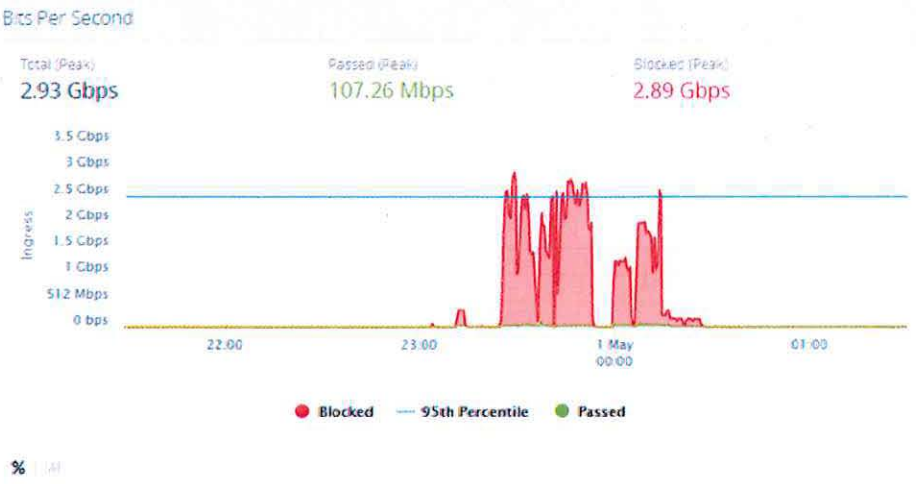
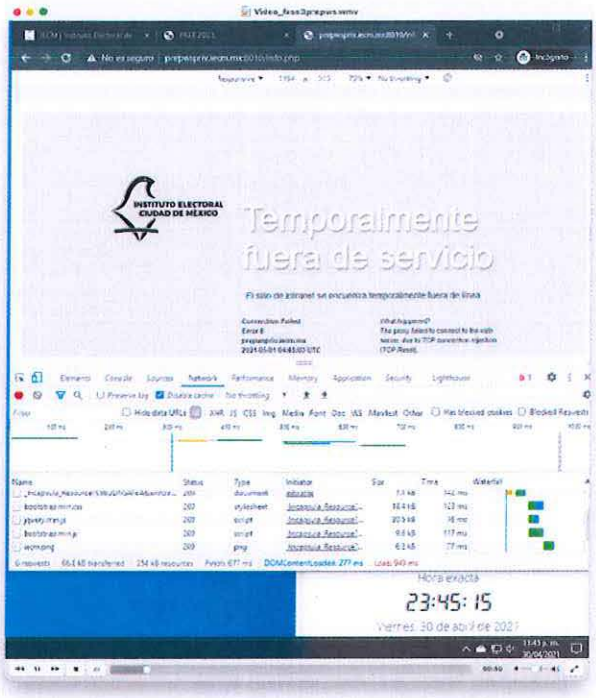


Ilustración 2.- Organización de la prueba.

Como resultado de la prueba se logró un tráfico de al menos Mbps y alcanzando un pico máximo de 293 Gbps.



El objetivo 1 y el objetivo 2 resistieron adecuadamente a las 5 fases del ataque, por otra parte, el objetivo 3 quedó fuera de servicio enviando el mensaje que se observa en la siguiente figura, este mensaje perduró durante toda la fase 3 de la prueba.

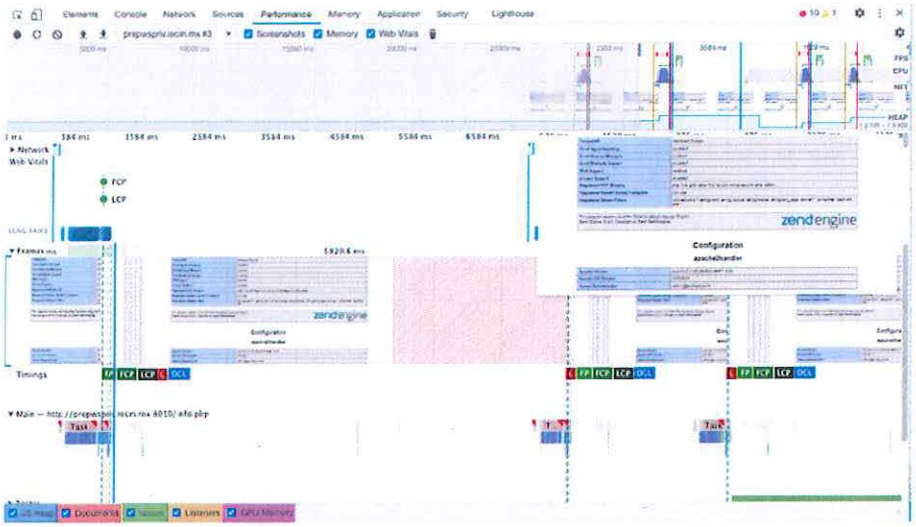


En ese momento se notificó al equipo de infraestructura del IECM quien realizó las remediaciones necesarias, que consistieron en aumentar el aprovisionamiento de memoria RAM a 128 GB y a 16 procesadores virtuales al servidor afectado.

Posterior a la remediación se repitió la prueba solo para el servidor con hallazgo, con el objetivo de comprobar que la remediación era la adecuada. Dándonos como resultado un tiempo promedio de respuesta de 0.96 segundos y cargando adecuadamente el contenido esperado.

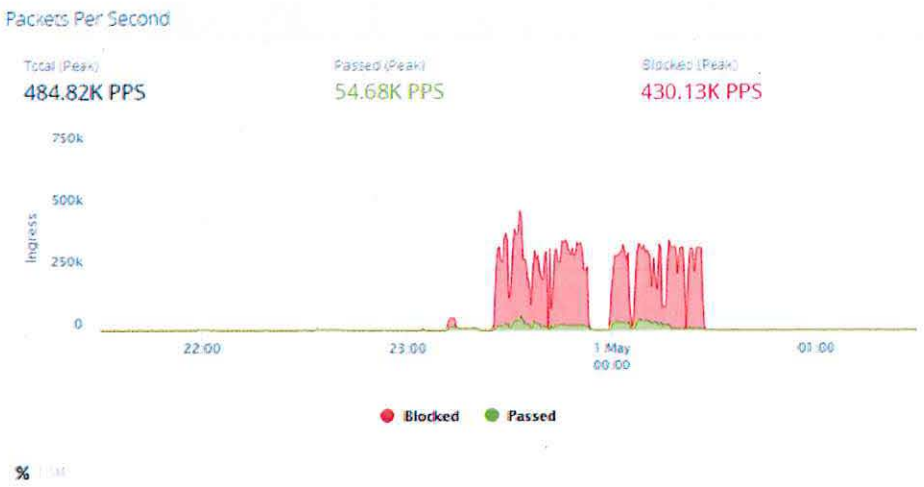
Sitio	DoS	Tiempos promedio
prepwspriv.iecm.mx:8010	00:012 a 00:23	0.96 segundos

Se realizó un perfilamiento del desempeño con la herramienta Performance de las DevTools del navegador Chrome y se observó que a partir de los 584 ms la página se encontraba ya renderizada por el navegador.



Se continuó la prueba hasta completar los 11 minutos y se comprobó que la remediación fue la adecuada.

En cuanto a los paquetes recibidos por segundo, la prueba logró un pico de hasta 484 mil peticiones por segundo, de los cuales la gran mayoría fueron bloqueados al tener un pico de 430 mil peticiones por segundo bloqueadas.



Conclusiones del ataque DoS

El hallazgo reportado durante las pruebas fue solventado de forma adecuada y revisada para comprobar su efectividad, dando como resultado que las medidas de remediación fueron correctamente implementadas.

La infraestructura aprovisionada para la solución PREP y los servicios de protección contratados, demostraron la capacidad de respuesta rápida al resolver el hallazgo en cuestión de minutos.

Las pruebas orientadas desde una perspectiva cuantitativa, nos proporcionó información necesaria para determinar el aspecto cualitativo de protección de los objetivos (prep2021.iecm.mx:8010, www.iecm.mx y prepwspriv.iecm.mx:8010) son los adecuados y nos permite concluir que tanto el sistema PREP, como el portal principal del IECM se encuentran adecuadamente protegidos contra ataques de negación servicio (DoS) para el día de la jornada electoral del 6 de junio del año 2021 y los días que dure el sistema en operación.

E) Resultados de la revisión del plan de seguridad.

Se realizó la revisión del plan de seguridad con base en los siguientes documentos proporcionados:

- Anteproyecto del plan de seguridad.
- Flujo de operación del PREP 2021.
- Plan de comunicación entre responsable e interesados.
- Plan de continuidad.
- Plan de mitigación.
- Análisis de riesgos.
- Baseline.

Donde se emitió únicamente la siguiente observación:

No se visualizó la definición de métricas/indicadores para monitorear el desempeño del

plan de seguridad planteado.

En cuanto al resto del plan, se concluye que en su conjunto, cumple con las buenas prácticas de la industría de la seguridad informática. Por lo cuál se da el visto bueno al plan de seguridad y continuidad para el Programa de Resultados Electorales Preliminares (PREP) 2021, del Instituto Electoral de la Ciudad de México. Los cuales cuentan con una buena documentación de las medidas de mitigación antes los riegos potenciales de los activos del IECM, muestra quienes están encargados para cada área en la cual puede tener algún incidente, al igual de un buen documento en la cual se registra la bitácora de incidentes, con esto se concluye que cumple con las medidas necesarias para la mitigación de incidentes en un corto periodo de tiempo.

F) Revisiones de seguridad adicionales.

Cómo parte de la revisión, se atestiguó la presentación de 3 herramientas de seguridad implementadas por el Instituto Electoral de la Ciudad de México, estas son:

Kiwi SysLog.

IECM presentó la consola web del sistema Kiwi en donde se observan los eventos de sistema e infraestructura.

Se observó que, en el caso del firewall principal, registra todos los niveles de eventos sin restricción, al ser un activo con alta importancia. En el caso del resto de activos los eventos se encuentran configurados para registrar de nivel Warning hacia arriba por cuestiones de desempeño, lo cual se considera una medida adecuada.

Se observó la posibilidad de crear filtros de exploración de eventos y el procedimiento para la exportación de los mismos.

Monitor de red PRTG.

IECM presentó el sistema de monitoreo de activos de red en donde se pudieron observar las prestaciones de la herramienta, dentro las que destacan:

a. Monitoreo de disponibilidad de servidores en tiempo real.
b. Monitoreo de uso de memoria en servidores.
c. Monitoreo de uso de capacidad de procesadores.
d. Monitoreo de espacio disponible en unidades de almacenamiento secundario y sus particiones.
e. Monitoreo del comportamiento y disponibilidad de red.

Durante la presentación se realizó una exploración de todas estas características.

Plataforma de seguridad Wazuh.

IECM presentó la implementación de la plataforma de seguridad Whazu en su infraestructura, en donde se pudo observar que es usado para recolectar datos de seguridad para ser analizados y monitorear el nivel de cumplimiento.
En la anterior imagen se observan diversos criterios de cumplimiento, dentro de los cuales sobresale el CIS Benchmark para RedHAt 7. El cual fue comparado con las pruebas realizadas con Nexpose y mostraron una diferencia que fue reportada.
Se mostró la implementación del monitor de integridad de archivos en los activos, se explicó a detalle su funcionamiento y se ejemplificó realizando cambios en dos archivos, se observó que la herramienta registró los eventos de modificación como se esperaba.
Cabe mencionar que esta capacidad de la herramienta Wazuh se puede combinar con el monitoreo antes mencionado, con el objetivo de identificar amenazas o servidores comprometidos durante la operación del sistema.

G) 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 nos 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 2021 (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.
E	Deuda Técnica" superior al 100%. Se requieren correcciones mayores 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.

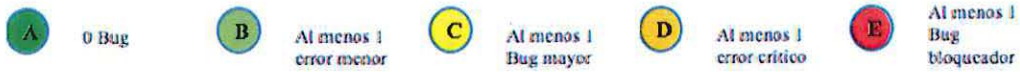
Bloqueante	Errores con una alta probabilidad de impactar en el comportamiento de las aplicaciones en producción: pérdida de memoria, conexión a BD no cerrada.
Critica	Errores con una baja probabilidad de impacto en el comportamiento del sistema o un tema que representa un fallo de seguridad: bloque catch 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

Página web de visualización de actas por capturar o validar

Fiabilidad: Incluye las evidencias de tipo bug y vulnerabilidades. Un bug representa algo que está mal en el código.

Numero de Bugs	Evaluación de fiabilidad	Esfuerzo de corrección
12	C	2 h 50 min



Seguridad: Incluye las evidencias de tipo vulnerabilidad, que representan una potencial para atacantes.

Vulnerabilidades	Evaluación de seguridad	Esfuerzo de corrección en seguridad
1	D	5 min

Mantenibilidad: Incluye las evidencias de tipo code smells, que son todas esas malas prácticas que a la larga van a provocar que cada vez sea más difícil hacer cambios en el código.

Code Smells	Evaluación de mantenibilidad	Deuda Técnica	Relación de la deuda Técnica	Esfuerzo para Alcanzar la Capacidad de Mantenimiento
35	A	2 h 44 min	0.1 %	0

Duplicado: Incluye información sobre líneas de código, bloques y archivos duplicados.

0.0 %	Bloques duplicados	0
	Líneas duplicadas	0
	Archivos duplicados	0

Tamaño: Número total de líneas de código, sentencias, funciones clases, etc.

Líneas totales	11,347
Sentencias	3,873
Funciones	644
Clases	0
Archivos	15
Directorios	4
Líneas comentadas	1,658
Porcentaje de líneas comentadas	18.1 %

Complejidad: Análisis del código para calcular la complejidad ciclomática. Cuando el flujo de una función se altera, es decir, se produce un salto, este contador incrementa.

Complejidad	2,961
Complejidad / Función	4.6
Complejidad / Archivos	269.2
Complejidad /Clases	0.4
Archivos	15
Directorios	4
Líneas comentadas	1,658
Porcentaje de líneas comentadas	18.1 %

Evidencias: Malas prácticas (violaciones de código).

Evidencias Encontradas	48
Evidencias confirmadas	0
Falsos positivos	0

Observaciones:

Se encontraron doce bugs en el código, sin embargo, fueron falsos positivos ya que se encuentran en el archivo jquery.js que contiene código de librerías de terceros.

Con respecto a las vulnerabilidades, se encontró una, sin embargo, también fue un falso positivo porque se encuentra en el archivo jquery.js.

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.

Sistema de captura y validación PREP 2021

El código del sistema de captura y validación PREP 2021 fue revisado manualmente en busca de posibles bugs y vulnerabilidades de seguridad, habiendo encontrado cuatro de las últimas, las cuales fueron reportadas y atendidas.

H) Revisión del Código fuente del sistema PREP Casilla.

Introducción

Este informe contiene los resultados de la revisión del código fuente y del archivo de aplicación (apk) de la aplicación móvil PREP-Casilla.

La revisión del código de la aplicación móvil y del archivo APK fue realizada utilizando dos herramientas que analizan el código y los archivos de la aplicación de manera

automática y los hallazgos verificados manualmente.

Objetivo general

Revisar el código fuente de la aplicación móvil del Programa de Resultados Electorales Preliminares 2021 (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 la aplicación ni que existan vulnerabilidades de seguridad.

Revisión del código fuente

1. ***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 tanto de seguridad como de buenas prácticas en la

E	programación. Es necesario revisar si estos errores obtenidos son falsos positivos y que estos no afecten el funcionamiento del sistema.

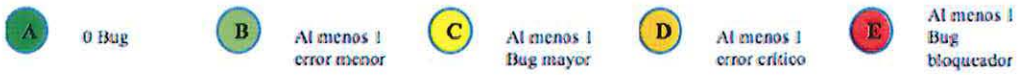
Evidencias: Número de "malas prácticas" (violaciones) en el código. Por ejemplo, números mágicos, llamar a un método que no es un constructor con el mismo nombre que una clase etc.

Bloqueante	Errores con una alta probabilidad de impactar en el comportamiento de las aplicaciones en producción: pérdida de memoria, conexión a BD no cerrada.
Critica	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.

2. ***Resultados de la revisión de código***

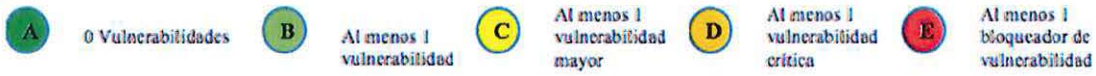
Fiabilidad: Incluye las evidencias de tipo bug y vulnerabilidades. Un bug representa algo que está mal en el código.

Numero de Bugs	Evaluación de fiabilidad	Esfuerzo de corrección
2	C	25 min



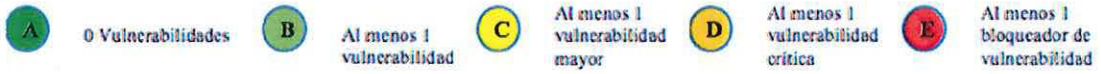
Seguridad: Incluye las evidencias de tipo vulnerabilidad, que representan una potencial para atacantes.

Vulnerabilidades	Evaluación de seguridad	Esfuerzo de corrección en seguridad
358	E	11 d



Mantenibilidad: Incluye las evidencias de tipo code smells, que son todas esas malas prácticas que a la larga van a provocar que cada vez sea más difícil hacer cambios en el código.

Code Smells	Evaluación de mantenibilidad	Deuda Técnica	Relación de la deuda Técnica	Esfuerzo para Alcanzar la Capacidad de Mantenimiento
14,329	B	95 d	5.0 %	1 h 32 min



Duplicado: Incluye información sobre líneas de código, bloques y archivos duplicados.

69.1 %	Bloques duplicados	644
	Líneas duplicadas	39,383
	Archivos duplicados	32

Tamaño: Número total de líneas de código, sentencias, funciones clases, etc.

Líneas totales	56,981
Sentencias	530
Funciones	46
Clases	351
Archivos	291
Directorios	272
Líneas comentadas	17,670
Porcentaje de líneas comentadas	36.6%

Complejidad: Análisis del código para calcular la complejidad ciclomática. Cuando el flujo de una función se altera, es decir, se produce un salto, este contador incrementa.

Complejidad	143
Complejidad / Función	2.0
Complejidad / Archivos	3.3
Complejidad /Clases	0.4
Archivos	291
Directorios	272
Líneas comentadas	17,670
Porcentaje de líneas	36.6%

comentadas	

Evidencias: Malas prácticas (violaciones de código).

Evidencias Encontradas	14,689
Evidencias confirmadas	0
Falsos positivos	0

Observaciones: Se encontraron dos bugs en el código, sin embargo, estos eran falsos positivos porque las excepciones a las que el sistema era propenso fueron evitadas en líneas previas. Con respecto a las vulnerabilidades, se encontraron 358, de las cuales 352 fueron falsos positivos, ya que se encontraron variables públicas en los archivos R.java, los cuales son generados automáticamente. El resto de las observaciones fueron atendidas por el Instituto.

Conclusiones de la revisión de la aplicación móvil

La aplicación móvil es adecuada para su uso el día de la jornada electoral del 1ero de julio de 2021, el sistema es seguro, hace lo que debe hacer y nada más.

I) 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 2021.

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	Solo uno
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 acceso a un site alterno.

En general se pudo comprobar que las instalaciones de cómputo y comunicaciones son adecuadas para soportar la ejecución del sistema PREP 2021.

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**) 2021 del Instituto Electoral de la Ciudad de México, 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 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.

El sistema **"PREP"** del Instituto Electoral de la Ciudad de México está en condiciones adecuadas para operar durante la jornada electoral del 6 de junio de 2021.

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