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

Auditoría Informática al Programa de Resultados Electorales Preliminares PREP 2018 para el IEEM

Informe final de la Auditoría de Software

Periodo de evaluación: del 14 de mayo al 28 de junio de 2018

Bitácora de modificaciones

Historia de versiones

Versión	Fecha	Descripción del cambio	Autor
0.0.1	02/abril/2018	Creación del formato.	René Dávila
0.1.0	14/mayo/2018	Estructuración Rubros	Marco Díaz
0.2.1	16/junio/2018	Pruebas funcionales de caja negra	Isaac Victoria
0.3.0	20/junio/2018	Análisis de vulnerabilidades a la infraestructura tecnológica	Fernando Lira
0.4.0	20/junio/2018	Pruebas de negación de servicio	Ángel Moreno
0.5.0	20/junio/2018	Validación del sistema informático del PREP y de sus bases de datos	Edgar Morales
0.5.1	21/junio/2018	1era Revisión	Ariadne Olarte
0.5.2	22/junio/2018	2da Revisión	Ulises de la Cruz
0.6.0	23/junio/2018	Revisión general	Jesús Hernández
0.6.1	28/junio/2018	3ra Revisión	Ulises de la Cruz
1.0.0	29/junio/2018	Revisión final	Jesús Hernández

1. OBJETIVO GENERAL 2
2. OBJETIVOS ESPECÍFICOS 2
3. ALCANCES 3
4. METODOLOGÍA 3
5. Resultados de la auditoría 5
A) Pruebas funcionales de caja negra al sistema informático del PREP. 5
Introducción 5
Metodología 6
Criterios utilizados para la auditoría 9
Resultados 9
B) Revisión del código fuente 14
C) Validación del sistema informático del PREP y de sus bases de datos. 16
Objetivo 16
Alcance 16
Procedimiento descrito de la firma del sistema PREP 16
✓ Obtención de firma previa a la elección (previo a la ejecución del PREP) 16
✓ Corroboración de firma el día de la elección (previo a la ejecución del PREP) 16
✓ Corroboración de firma el día de la elección (durante la ejecución del PREP) 16
✓ Corroboración de firma el día de la elección (posterior a la ejecución del PREP) 17
Procedimiento de verificación de la App PREP IEEM 18
Procedimiento para la verificación de la Base de Datos (debe estar en cero) 18
✓ Identificación de tablas de base de datos 18
✓ Verificación de bases de datos en cero 18
D) Análisis de vulnerabilidades a la infraestructura tecnológica 19
Objetivos 19
Alcance 19
Pruebas de penetración (pentest) 20
Revisión de configuraciones 22
E) Pruebas de negación de servicios. 23
Objetivo 23
Alcance 23
Resultados 24
Conclusión de la prueba de Negación de Servicio: 26
6. Dictamen de la auditoría 27

1. OBJETIVO GENERAL

Realizar una auditoría informática al Programa de Resultados Electorales Preliminares (PREP) 2018, del Instituto Electoral del Estado 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 solo 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 14 de mayo al 28 de junio de 2018.

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 – IEEM, en CISA de ISACA 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 está basada en lo general, en el proceso de auditoría que establece el manual CISA (Certified Information System Auditor) de la Information System Audit and Control Asociation (ISACA) en concordancia con la metodología propuesta en el instrumento jurídico celebrado entre "La UNAM" y "El IEEM", cuyo objetivo general es aplicar los estándares de auditoría de Sistemas de información con el fin de realizar una auditoría en cualquier área de Tecnología de la Información de forma profesional.
La metodología está basada en análisis de riesgos e inicia con la comprensión de los objetivos primordiales del Instituto Electoral del Estado de México, con el objetivo de identificar los activos importantes y riesgos basados en lo siguiente:

1. Recopilación de información del Instituto Electoral del Estado de México.
2. Realizar un análisis de riesgos y ajustar el plan de la auditoría.
3. Obtención de elementos de control interno.
4. Realizar pruebas de cumplimientos.
5. Realizar entrevistas para identificar riesgos.
6. Revisión de la infraestructura.

7. Pruebas de penetración
8. Recabar evidencia y escribir recomendaciones.

De forma particular se emplearon las siguientes metodologías: La metodología utilizada para la revision de la calidad de software 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 de seguridad la 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 IEEM originado a raíz de las pruebas realizadas.

Los resultados se muestran 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 App PREP IEEM. Para lo cual, se considera lo descrito en el Anexo 13 de los Lineamientos

Operativos del Programa de Resultados Electorales Preliminares 2018; 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 App PREP IEEM. 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 25 al 31 de mayo de 2018 y revisiones posteriores para dar seguimiento a las remediaciones.

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 PREP Casilla 2018 IEEM	
	Institución:	Universidad Nacional Autónoma de México Facultad de Estudios Superiores Aragón Centro Tecnológico Aragón	
No. Caso de prueba:	01	Nombre:	Login Correcto

Diseñado por:	Angel Blas, Eduardo Bolaños
Probado por:	
Fecha de la prueba:	
Tipo de prueba:	Software
Precondiciones:	Haber realizado el registro de un usuario en Base de Datos. Tener un nombre de usuario y una contraseña asignados por la UIE. Haber ejecutado el aplicativo "PREP-IEEM" en el dispositivo Android
Descripción de la prueba:	Se verificarán los flujos principales del caso de uso para realizar el acceso al sistema.

Elemento (s) a ser probado		
1		Reconocimiento del usuario basado en un usuario y una contraseña.
2		Verificación de la información en la base de datos.
3		Verificación de información de usuario en la bitácora.

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

Hardware: Dispositivo Android configurado por el personal de la UIE con acceso al sistema PREP.

Software: Aplicativo "PREP-IEEM".

Base de datos: Se requiere un usuario con privilegios de sólo lectura sobre las tablas de usuarios y bitácoras.

Especificaciones

Entrada	Resultado esperado	Resultado obtenido
- Ingresar a BD tabla usuario	-Existe la información del usuario que va a ingresar al sistema. Nota: La contraseña se encuentra "en claro"	
- Ingresar en BD tabla bitácora	-No exista el registro del usuario que se va a ingresar al sistema.	
- Nombre de usuario correcto Contraseña correcta	-Que el sistema identifique de forma correcta al usuario por nombre de usuario y contraseña. -Acceso al menu principal del sistema. -Que el sistema registre en la bitácora el acceso que se realiza.	

	Proyecto:	Auditoria PREP Casilla 2018 IEEM	
	Institución:	Universidad Nacional Autónoma de México Facultad de Estudios Superiores Aragón Centro Tecnológico Aragón	
No. Caso de prueba:	01	Nombre:	Login Correcto

	Pasos a seguir	Check
1	Ingresar a BD tabla usuario y verificar si existe la información del usuario que va a ingresar al sistema. Nota: Verificar si la contraseña se encuentra "en claro"	√
2	Ingresar a la BD que contiene la bitácora de acceso y verificar que no exista el registro del usuario que se va a ingresar al sistema.	/
3	Ingresar a la aplicación "PREP-IEEM". Verificar que la pantalla muestre el formulario de inicio de sesión con el mensaje "PREP-IEEM", con los componentes. - Campo de tipo texto para ingresar un usuario con la etiqueta "Usuario". - Campo de tipo password para ingresar una contraseña con la etiqueta "Contraseña". - Botón con la etiqueta "INGRESAR".	/
4	Ingresar el nombre de usuario y contraseña (10 dígitos, numero, letras y simbolos especiales) en sus campos correspondientes y pulsar el botón "INGRESAR"	/
5	Verificar el acceso al sistema donde se muestre el menú principal del aplicativo.	/
6	Ingresar a la base de datos con el usuario de lectura sobre la tabla de bitácoras y verificar que exista el registro del usuario que se firmo.	/
7	Verificar que el usuario sólo tenga acceso a las funcionalidades de acuerdo con su perfil.	/
8	Salir de la aplicación y verificar que los datos de la sesión se hayan borrado	/
9	Intentar ingresar utilizando otro usuario. Repetir el paso 4	/
10	Verificar que no se dé acceso al menú principal con el nuevo usuario. El dispositivo se asigna unicamente al primer usuario que accede al sistema.	/

Auditor **Representante IEEM**

Nombre y Firma

Nombre, cargo y Firma

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

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

	Documentos solicitado	Entregados	No entregado
IEEM	22	22	0

El Instituto Electoral del Estado de México cumple con todas las etapas mínimas para el desarrollo del sistema PREP descritas en el Anexo 13, título II, capítulo II, numeral 4. Dichas etapas se enlistan a continuación:

Documento	Cumple
Análisis	Sí
Diseño	Sí
Construcción	Si
Pruebas	Sí

Estas etapas son las fases por las que pasa un sistema informático para resolver un problema:

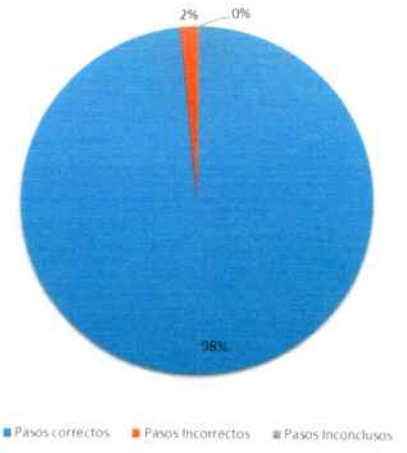
- Entender el problema (análisis)
- Plantear soluciones (diseño)
- Llevar a cabo la solución
- Realizar pruebas

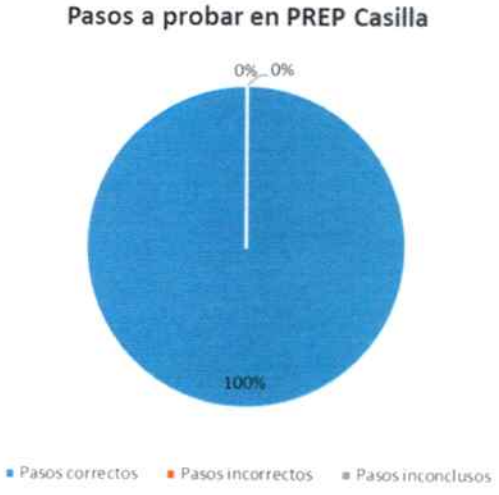
Las pruebas de funcionalidad se realizaron a través de 31 casos de prueba, en ellos se establece el funcionamiento técnico operativo del sistema PREP y App PREP IEEM. Cada caso de prueba contiene un número de pasos que, a ser revisados, para dichas pruebas se estableció un total de 428 pasos, los cuales resultan en un estatus:

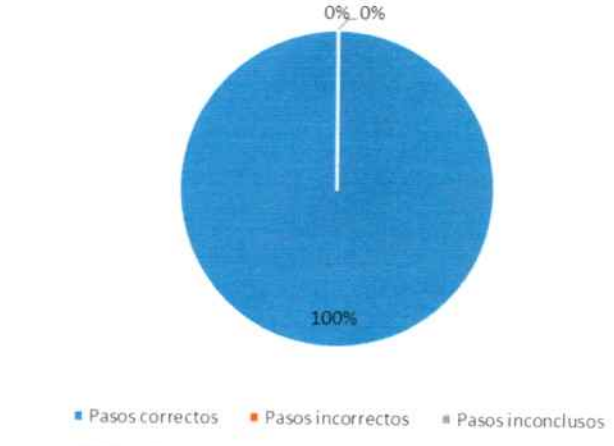
- Correcto. - Al ejecutar el paso, el resultado esperado es igual al resultado obtenido.
- Incorrecto. - Se ejecuta el paso y el resultado obtenido es distinto al esperado.
- Inconcluso. - Se ejecuta el paso, sin embargo, por falta de información no se puede observar el resultado para compararlo con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

	Pasos a probar	Correctos	Incorrectos	Inconclusos
PREP	279	272	7	0
App PREP IEEM	149	149	0	0
Total	428	421	7	0

Gráfica general de pasos a probar de PREP y PREP Casilla







De la ejecución de casos de prueba se obtuvo que la mayoría de los pasos realizados calificaron como correctos (un 98%), lo cual deja fuera un 2%(7 casos de prueba), que se deben a errores de diseño en la parte de la publicación donde la página no se adapta al 100% al tamaño de la pantalla para dispositivos móviles; por lo tanto, esto no afecta en nada al correcto funcionamiento del sistema.

Se realizó la visita al CCV central en los tres simulacros y de 5 CATD para el tercer simulacro. Se observó que la organización del equipo de cómputo en todas las locaciones es adecuada.

En el CCV los capturistas debían esperar la llegada de un acta al sistema para posteriormente capturarla.

Primer Simulacro

Se visitó el CCV principal, dónde se realizó la simulación de un corte de energía para verificar el funcionamiento de la planta eléctrica, se realizaron dos cortes:

	Primer corte		Segundo corte	
	Se mantienen	Se apagan	Se mantienen	Se apagan
CCV principal	96	64	103	57

Se realiza la observación de que el sistema, aunque funcionó, operó de manera lenta durante el simulacro. En este simulacro se tomaron tiempos tanto de llegada del acta como de captura o verificación. Se tuvo un promedio de 1 minuto 55 segundos para los tiempos de llegada y de 1 minuto 1 segundo para los de captura o verificación.

Segundo Simulacro

Se visitó el CCV principal.

Se realiza la observación de que el sistema, aunque funcionó, operó de manera lenta durante el simulacro. En este simulacro se tomaron tiempos tanto de llegada del acta como de captura o verificación. Se tuvo un promedio de 2 minutos 7 segundos para los tiempos de llegada y de 38 segundos para los de captura o verificación.

Tercer Simulacro

Se visitó el CCV principal y 4 CATD.

Se realiza la observación de que el sistema, aunque funcionó y mostró mejoras en el tiempo, se considera que la velocidad de este aún debería mejorar. En este simulacro se tomaron tiempos de captura o verificación. Se tuvo un promedio de 40 segundos para los de captura o verificación.

En los CATD únicamente se digitalizaron actas de escrutinio y cómputo (AEC), proceso que se realizó de manera eficiente y rápida. Aunque de existir problemas de red es probable que actas ya digitalizadas tarden un poco en ser enviadas.

Se tomó el tiempo promedio de digitalización en 4 distritos, estos fueron:

- 6 segundos en el distrito V
- 10 segundos en el distrito VI
- 4.87 segundos en el distrito XLII

- 9 segundos en el distrito III

Durante la revisión de las pruebas funcionales de caja negra se encontraron varios hallazgos, a continuación, se describe el número y su estatus.

	Primer simulacro	Segundo simulacro	Tercer simulacro
Hallazgos en PREP	3	2	2
Hallazgos en App PREP IEEM	0	0	0
Total	7		

Hallazgos durante los simulacros:

- 1er simulacro
  - Inconsistencia en imágenes y datos publicados. Durante el simulacro se verificó la base de datos para determinar en donde estaba el error, se comprobó que las bases de datos se encontraban con información correcta y que el error se trataba de un problema de transformación de datos para la publicación. Fue reportado y verificado en el segundo simulacro.
  - Actas mal capturadas, fue reportado y verificado al siguiente simulacro.
  - Avance de publicación muy lento, se reportó y verificó en el siguiente simulacro.
- 2° simulacro
  - Las inconsistencias el primer simulacro fueron arregladas.
  - Ya no aparecieron imágenes mal capturadas.
  - El sistema permaneció lento, el porcentaje de avance era similar al primer simulacro. Se reportó y se verificó en el tercer simulacro.
- 3er Simulacro
  - Se detectaron actas de un ejercicio previo, se emitieron recomendaciones y fueron verificadas el día 28 de junio como se explica en los párrafos de abajo.
  - El sistema permaneció lento y con dos cortes sin reflejar avances. Se emitieron recomendaciones y se verificaron en el ejercicio del 28 de junio dando muy buenos resultados como se explica en los párrafos a continuación.

También se verificó el código fuente a fin de conocer que el sistema no contenga vicios

ocultos o malas prácticas que pongan en riesgo el rendimiento o la seguridad del sistema.

B) Revisión del código fuente

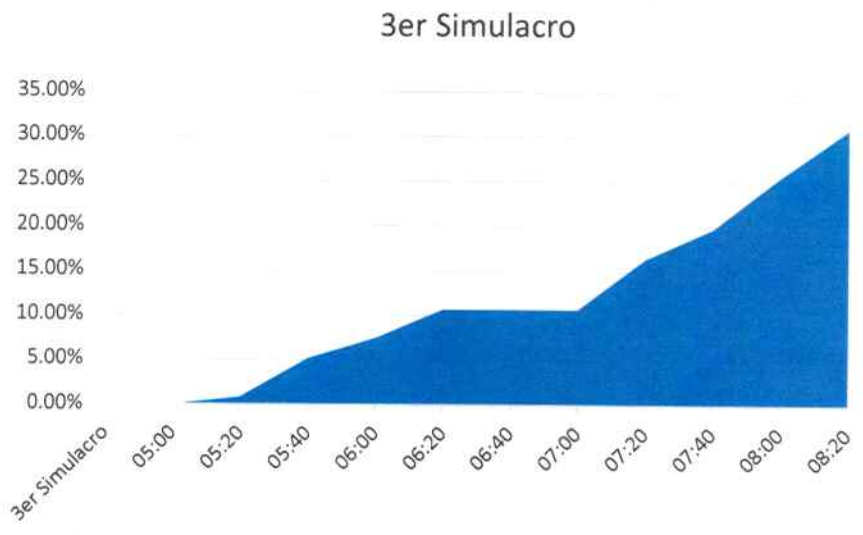
Para la verificación de código fuente se nos proporcionó la carpeta del proyecto, realizamos la verificación y encontramos lo siguiente:
La primera verificación fue comprobar que el código correspondía a las funcionalidades del proceso técnico operativo, y que no existiera código adicional al código que implementa esas funcionalidades. Dando como resultado que en efecto el sistema no hace nada más para lo que fue diseñado.

En el módulo de captura verificamos la calidad del código, encontramos que la programación es adecuada y no cuenta con problemas de seguridad. La programación plasmada ahí, denota la experiencia de años de programación en las tecnologías seleccionadas para este desarrollo.

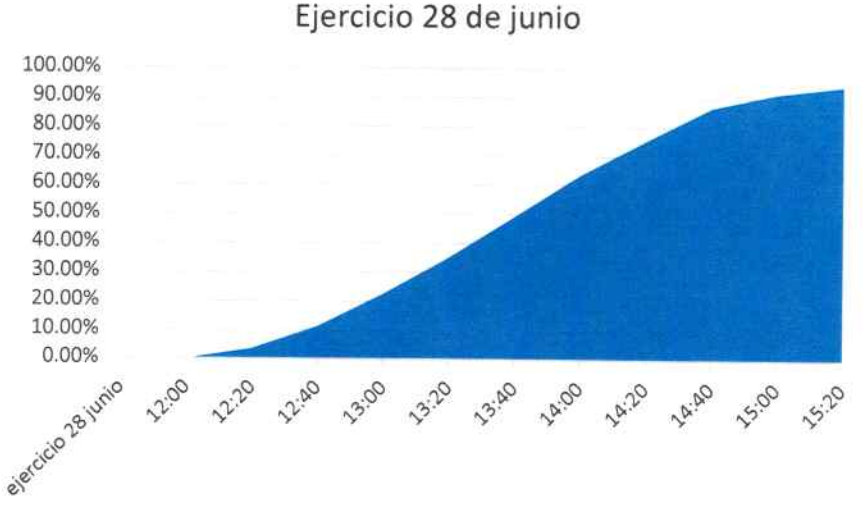
Detectamos que el código es heredado el cual tiene la ventaja de contar con código conocido y bien probado. Sólo con la observación que la tecnología de programación debe ser actualizada.

La implementación de conexión a bases de datos se encuentra correctamente implementada al emplear PoolConnections y buenas prácticas de programación. Sin embargo, se recomienda que se empleen procedimientos almacenados del lado del SGBD.

En el proceso de publicación revisamos la programación del proceso de copiado de las actas digitalizadas al servidor de publicación, encontramos que el código fuente para la transferencia de la información es adecuada, pero sin embargo consideramos que se desperdicia el ancho de banda por ser de forma secuencial. Al finalizar el 3er simulacro se recomendó la implementación de la transferencia por medio de hilos java. En este punto también llegamos al acuerdo de bajar la calidad de las imágenes de 1.2MB a 400KB, con el objetivo de mejorar el tiempo de transferencia. En el ejercicio del 28 de junio se revisó y nos encontramos con estas recomendaciones implementadas, dando como resultado una mejora en el avance del PREP como se observa en las gráficas a continuación.



3er simulacro que inicio a las 5 PM del día 24 de junio.



Ejercicio del 28 de junio para verificar implementación de recomendaciones, inició a las 12:00 horas.

En el que se puede observar una mejora significativa. En este mismo ejercicio se verificó la recomendación de validar las fechas de las actas, quedando solventado la validación dentro de la App. PREP IEEM, La validación de las actas del lado del servidor fueron realizadas el día 29 de junio en el servicio web de recepción de actas, se verificó el código fuente que realiza dicha validación; implementaron una función de validación y lógica de negocio para dicho fin. Esto permitirá descartar las actas que tengan una fecha fuera del rango esperado.

Se detectó que parte de los programas de publicación se involucran lenguajes de programación distintos a java, lo cual conlleva a un hallazgo de integración de los módulos, se recomienda ampliamente homologar las tecnologías de programación a través de capacitación en arquitecturas de software, patrones de diseño de Software y tecnologías de programación Java.

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

Objetivo

Validar que el sistema informático del PREP que operará el día de la Jornada Electoral, corresponda al software auditado, así como que la base de datos se encuentre sin registros adicionales a los necesarios para que el sistema opere. La validación respecto a la correspondencia del software auditado y el utilizado en la operación del PREP, se tendrá que realizar al inicio, durante y al final de la operación del sistema informático del PREP.

Alcance

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

Procedimiento descrito de la firma del sistema PREP

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

Una vez concluida la auditoría se realizará la firma del sistema PREP mediante la función SHA-256, para posteriormente hacer la comparación al mismo, el día 29 de junio se realizará dicha firma.

ii. 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 **i.** y la firma generada este día por el ente auditor, el notario verificará que las respectivas firmas coincidan.

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

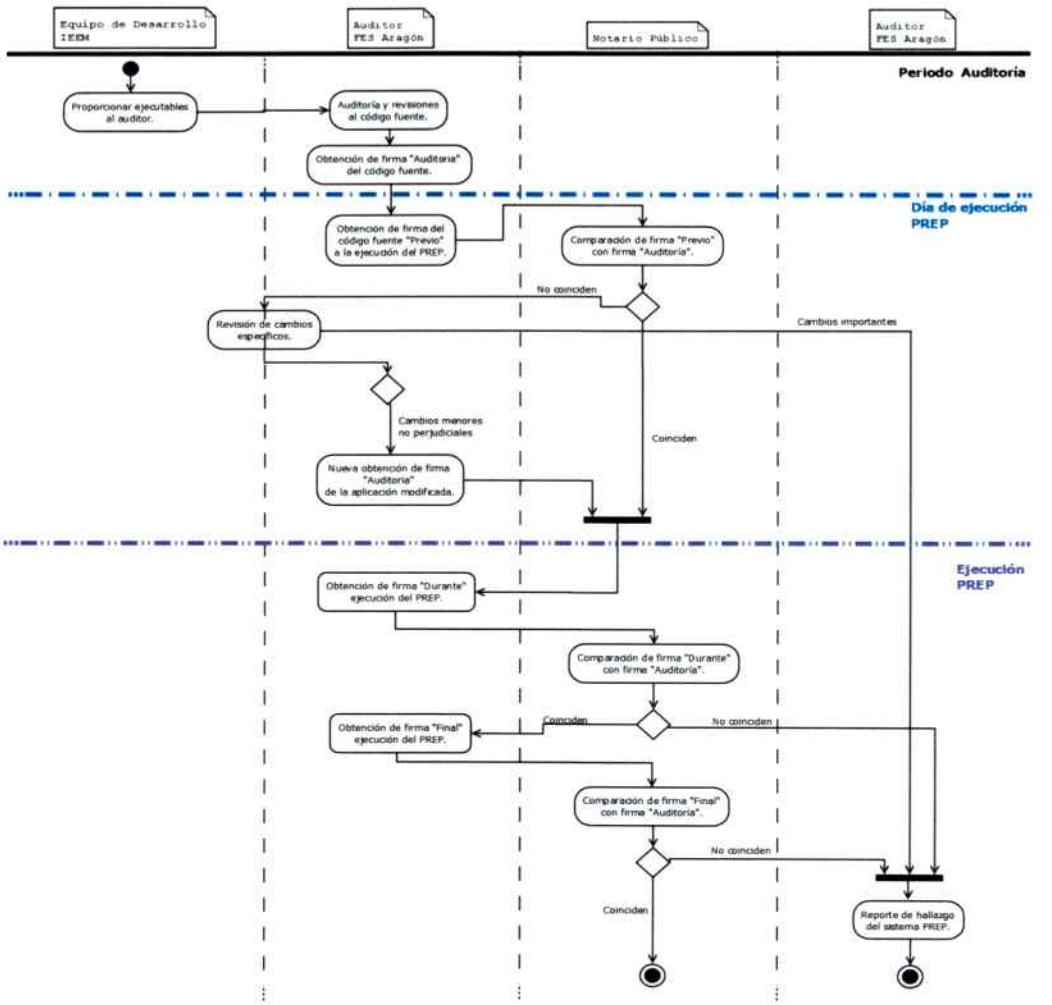
El día de la elección, mientras el sistema PREP se encuentra en ejecución, se

realizará una segunda verificación del software a través de la comparación de la nueva firma, y la firma obtenida en el punto, la verificación la hará el ente auditor.

iv. 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 **i.**, el notario verificará que las respectivas firmas coincidan.

Diagrama de flujo



Procedimiento de verificación de la App PREP IEEM

Debido a que los equipos Android de digitalización ya se encuentran distribuidos en todo el Estado de México, el procedimiento de verificación de la aplicación se hará el mismo día que se genere la llave del sistema PREP, revisaremos que la versión del sistema instalado en las tabletas Android por medio del archivo de identificación instalado sea el correspondiente a la compilación y al APK del sistema auditado. Si ese archivo no se encuentra dentro del sistema de archivos y con una clave específica, quiere decir que ese software no es la última versión y no permitirá al usuario emplear las funciones de digitalización. De esta forma podemos asegurar que el sistema auditado es la misma versión que se encuentra en ejecución.

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

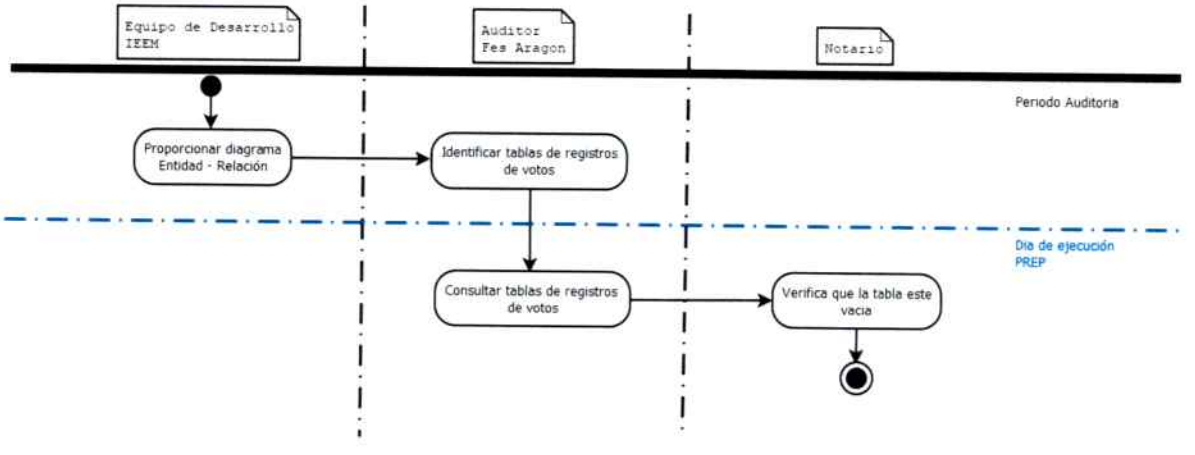
v. Identificación de tablas de base de datos

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 del Estado de México.

vi. Verificación de bases de datos en cero

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

Diagrama de flujo



D) 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 IEEM las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.

- Verificar que las medidas implementadas por el IEEM hayan atendido adecuadamente las vulnerabilidades reportadas.

Alcance

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

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

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

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 IEEM, puedan dar seguimiento a los mismos.

II. Validación de reporte de hallazgos. El IEEM 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 IEEM 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 IEEM pueda atender los hallazgos.

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

Pruebas de penetración (pentest)

1. Introducción

Las pruebas ejecutadas previo al primer simulacro del sistema PREP tuvieron como objetivo, la identificación anticipada de posibles vulnerabilidades que expongan al sistema y/o sus activos durante la ejecución del mismo. En esta primera etapa se realizó únicamente el descubrimiento y enumeración de recursos dentro de la infraestructura perteneciente al sistema.

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 telecomunicaciones, servidores y las aplicaciones web que en ellos residen, así como las estaciones de trabajo de captura y envío de 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	Menor	No se detiene ni afecta ningún proceso.
2	Medio	Procesos de baja prioridad se ven afectados, pero no detenidos.
3	Alto	Procesos de alta prioridad se ven afectados, pero no detenidos.
4	Crítico	Procesos de alta prioridad se ven afectados y pueden ser detenidos.

4. Técnicas y vectores de ataque

Durante las pruebas ejecutadas previo al primer simulacro se utilizaron técnicas de descubrimiento y escaneo basadas en diferentes protocolos para obtener información sobre el sistema que nos permita generar vectores de ataque con altas probabilidades de efectividad.

5. Resultado de las pruebas

Resultado de la verificación de la aplicación de las recomendaciones

En la fase de pruebas de seguridad de caja negra y de acuerdo al carácter de la fase de pruebas (descubrimiento), los hallazgos no corresponden a vulnerabilidades críticas del sistema, sin embargo, todos los hallazgos deben ser analizados y evaluados para su posterior mitigación o aceptación.

Se ejecutaron pruebas de escaneo de puertos, pruebas de vulnerabilidades, se revisó la configuración de la red, y el aislamiento de la misma.

En los CCV`s se observa que en su configuración de red no hay salida a internet, se verifico que no hay comunicación al siguiente nodo o computadora dentro del segmento de red sobre el que opera el sistema del Instituto y todo el tráfico se filtra por los equipos correspondientes.

Se encontraron dos hallazgos de impacto bajo y dos de impacto medio, los cuales fueron reportados al área correspondiente en el Instituto, mismos que fueron

subsanados adecuadamente.

En las pruebas de penetración de caja blanca, se nos permitió la conexión en la zona DMZ y se realizó un escaneo de vulnerabilidades, encontrando 1 crítica, y dos de impacto medio. Se reportaron en el momento y fueron solventadas en menos de dos días.

Revisión de configuraciones

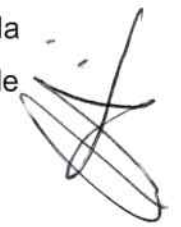
1. Objetivo

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

2. Alcance

La auditoría se realiza del 14 de mayo al 28 de junio de 2018.

Los alcances de este documento están establecidos en el Anexo Técnico en la sección III. Capitulo II Objetivos Específicos numeral 3, Sección "Para revisión de configuraciones"



3. Hallazgos

El hallazgo más importante en esta revisión fue el correspondiente a los reportados en las pruebas de penetración de caja blanca, en la cual algunos equipos eran vulnerables por falta de actualizaciones de seguridad y un par de equipos falta de endurecimiento (Hardening), los cuales fueron solventados de inmediato.

Se realizaron revisiones a las reglas de los diferente Firewall, revisiones a la configuración de la réplica de base de datos, inspección de las bitácoras del servidor de aplicaciones, revisión a los servidores de base de datos y servidores de aplicaciones, entre otros.

4. *Conclusiones de la revisión de las configuraciones*

Durante la revisión de las configuraciones de la infraestructura se reportaron los hallazgos junto con las recomendaciones correspondientes para la mejora de su configuración, los cuales fueron reportados y subsanados de manera adecuada.

E) 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 IEEM, 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 Instituto Electoral del Estado de México, 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.
- 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 Instituto Electoral del Estado de México efectué la contramedida para la mitigación.

Resultados

Recibimos la autorización para realizar estas pruebas el día 27 de junio, donde se nos proporcionó la URL objetivo de la prueba e indicándonos(verbalmente) que es la misma infraestructura en que estará operando el sitio principal del IEEM:

IEEM Julio 2018

Unidad de Informática y Estadística

Toluca de Lerdo, México, 27 de junio 2018
IEEM/UIE/714/2018

MAESTRO
MARCELO PÉREZ MEDEL
ACADÉMICO DEL LABORATORIO DE CÓMPUTO
CENTRO TECNOLÓGICO ARAGÓN, UNAM

Con la finalidad de dar cumplimiento al Programa de Infraestructura en Tecnologías de la información y Comunicaciones del Programa Anual de Actividades 2018, a los Lineamientos Operativos del PREP 2018, así como en alcance al Convenio de Colaboración UNAM-IEEM mediante el Centro Tecnológico Aragón de la Facultad de Estudios Superiores Aragón, respetuosamente le informo que con la finalidad de que se realicen las pruebas necesarias que forman parte de la Auditoría en Informática al Sistema PREP 2018, en específico a la infraestructura para la difusión de los resultados que en su momento, serán publicados en Internet por la empresa TELMEX, dicha empresa autoriza realizar las pruebas en el sitio público bajo el dominio **www.prepieem.org.mx** el día 28 de junio del presente en un horario de las 20:00 las 21:00 horas.
Le reitero la seguridad de mi consideración distinguida.

"TU HACES LA MEJOR ELECCIÓN"
ATENTAMENTE

JUAN JOSÉ RIVAUD GALLARDO
JEFE DE LA UNIDAD

c.c.p. Lic. Pedro Zamudio Godínez. Consejero Presidente.
c.c.p. Lic. Sandra López Bringas. Consejera Electoral y Presidenta de la CEPAPREP.
c.c.p. Mtro. Francisco Javier López Corral. Secretario Ejecutivo.
c.c.p. Archivo/Minutario

Una vez obtenido la autorización se realizó el ataque por medio de infraestructura de cómputo distribuida, reproduciendo las condiciones que un atacante real emplearía.

El ataque inició a las 20:00 y finalizó a las 21:00 y en todo momento un miembro de nuestro equipo se mantuvo monitoreando el sitio objetivo y realizando una grabación de video para contar con la evidencia necesaria. Unos minutos antes del ataque se dedicaron a registrar los tiempos de respuesta normales del sitio objetivo, registrando un valor de 880 milisegundos en promedio.

La ejecución de scripts y herramientas de ataque se iniciaron inmediatamente a las 20:00, observando poco después un incremento mínimo en el tiempo de la carga de

la página a 1.60 s en promedio. Para un tiempo estimado de 2s de carga a las 20:22, observando pequeños tiempos de carga, pero sin interrumpir el funcionamiento normal de la página. Siendo las 20:40 se observa un tiempo de carga de 1.61s. Concluyendo a las 21:00 hrs, se observó durante el ataque que la página http://www.prepieem.org.mx/ continuó operacional sin interrupción o incidencia.

Conclusión de la prueba de Negación de Servicio:

La infraestructura tecnológica implementada en el sitio web del PREP para el IEEM con URL: http://www.prepieem.org.mx/ cuenta con la adecuada protección contra ataques de Negación de Servicio y Ataques de Negación de servicio Distribuido al mantene en línea durante todo el ataque. Al ser la misma infraestructura para el sitio web principal, la que funcionará el día de la jornada Electoral pero con el dominio http://ieem.org.mx/. Esta conclusión aplica para esta URL también.

6. Dictamen de la auditoría

Como resultado de las pruebas y revisiones a los sistemas del "Programa de Resultados Electorales Preliminares" (PREP) 2018 del Instituto Electoral del Estado de México, manifestamos que:

- La implementación de la solución tecnológica y servidores asociados a los procesos del PREP 2018 son razonablemente seguros, su nivel de riesgo es muy bajo para la operación del servicio mencionado y se encuentran configurados adecuadamente para la operación.
- El sistema "PREP 2018" del Instituto Electoral del Estado de México es seguro: robusto, confiable, y cumple con los requerimientos funcionales del sistema, realizan 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.

El sistema "PREP 2018" del Instituto Electoral del Estado de México está en condiciones adecuadas para operar en las jornadas del día 1 de julio de 2018

M. en C. JESÚS HERNÁNDEZ CABRERA
Responsable de la auditoría