Casa abierta al tiempo

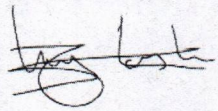
UNIVERSIDAD AUTÓNOMA METROPOLITANA
Unidad Iztapalapa

Auditoría de Verificación y Análisis del Sistema informático que será utilizado en la implementación y operación del Programa de Resultados Electorales Preliminares del IEEM

Informe Final de la Auditoría

1° de junio de 2023

Aprobación del Documento

Línea de Trabajo	Responsable	Firma
Coordinador General del Convenio	Ing. Luis Fernando Castro Careaga	

1° de junio de 2023

Historia de Cambios

Fecha	Versión	Autor	Descripción
31/05/2023	0.8	JMCV OLCJ ERF RMR LFCC	Elaboración y ajustes
27/04/2023	1.0	LFCC	Versión ajustada final revisada

Contenido

1. Informe Ejecutivo

El 1° de marzo del 2023, la UAM-I y el IEEM firmaron un convenio de colaboración para la ejecución de la "Auditoría de Verificación y Análisis del sistema informático que será utilizado en la implementación y operación de Programa de Resultados Electorales Preliminares (PREP)" teniendo como objetivo final validar ante la sociedad que el sistema informático del PREP es confiable y seguro.

La auditoría se realizó a través de 6 líneas de trabajo.

Pruebas funcionales de caja negra (PFCN)

> Las PFCN consisten en usar de una manera estructurada las funciones del sistema informático y validar que su comportamiento es como se espera de acuerdo con sus especificaciones y al Proceso Técnico Operativo, sin tomar en cuenta la forma en que está construido.
>
> Se realizaron 3 ciclos de prueba aplicándose múltiples casos de prueba para asegurar que el sistema funciona como se espera. Los hallazgos encontrados por el equipo de la UAM-I fueron notificados al equipo del IEEM, el cual los atendió. El equipo de la UAM-I verifico su correcta resolución.
>
> De los resultados de las PFCN puede afirmarse que el sistema informático del PREP funciona como se espera y no tiene funciones que no estén dentro de sus especificaciones.

Validación del sistema informático (VSI)

> La VSIBD tiene como objetivo asegurar que el sistema informático usado para el PREP es el mismo que fue auditado, así como asegurar que al iniciar la operación del PREP, este inicializado correctamente y no existan actas precargadas.
>
> Para hacer la validación se desarrolló un Módulo de Validación que permite hacer las validaciones previo al inicio de operaciones, durante la operación y al cierre de operaciones del PREP.
>
> Este módulo será utilizado los días de 4 y 5 de junio para las actividades de la VSI.

Análisis de Vulnerabilidades (AV)

> El AV tiene como objetivo identificar las vulnerabilidades de seguridad del sistema informático del PREP. Esté análisis se hace mediante la identificación de todos los

elementos de Tecnología de Información y Comunicaciones (TIC) del sistema informático del PREP, hacerles una revisión a las configuraciones de cada elemento, identificar las vulnerabilidades de estas y aplicar pruebas de penetración para validar los hallazgos y probar el comportamiento de la infraestructura tecnológica del PREP. Se realizaron dos ciclos de pruebas de penetración.

Los hallazgos encontrados por el equipo de la UAM-I fueron notificados al equipo del IEEM, el cual los atendió. El equipo de la UAM-I verifico su correcta resolución.

De los resultados de la AV se puede afirmar que el sistema informático del PREP no cuenta con vulnerabilidades relevantes que pongan en riesgo su operación.

Auditoria al Código Fuente (AC)

La AC tiene como objetivo validar que la programación del sistema informático del PREP no contiene instrucciones que pudieran generar una vulnerabilidad de seguridad.

El código del PREP se sometió a herramientas especializadas de búsqueda de patrones de programación de riesgo.

Los hallazgos encontrados por el equipo de la UAM-I fueron notificados al equipo del IEEM, el cual los atendió. El equipo de la UAM-I verifico su correcta resolución.

De los resultados de la AC se puede afirmar que el sistema informático del PREP no cuenta con patrones de programación en su código que pongan en riesgo su operación.

Pruebas de Negación de Servicio (PNS)

Las PNS tienen como objetivo aplicar al sitio de publicación del PREP y al sitio institucional del IEEM, flujos de mensajes que simulen ataques informáticos reales, y validar que son capaces de detectarlos y son resilientes a los mismos.

Se aplicó un primer ciclo de PNS y se encontró un hallazgo. La resolución del hallazgo siguió un ciclo: atención del hallazgo por el IEEM y una aplicación de la PNS para validar su corrección. Dada la complejidad del hallazgo, fueron necesarios 3 ciclos de resolución para validar que el hallazgo había sido resuelto.

De la aplicación de las PNS se puede asegurar que el sitio de publicación de resultados del PREP y el sitio institucional del IEEM resisten ataques de negación de servicio como los especificados en el Anexo Técnico.

Revisión del Apego del Sitio de Publicación (RASP)

La RASP tiene como objetivo asegurar que el sitio de publicación de resultados del PREP sigue la normatividad de las plantillas proporcionadas por el INE. Esta revisión se aplicó tanto al sitio de navegador en escritorio como al sitio en su versión para dispositivo móvil.

Se realizaron 3 ciclos de RASP los cuales detectaron hallazgos menores. En el último ciclo de RASP se encontraron elementos fuera de la plantilla del INE mismos que al ser notificados al personal del IEEM, comunicaron que no serían atendidos.

No considerando el hallazgo señalado, a partir de la RASP realizadas se puede asegurar que el sitio de publicación en sus dos versiones se apega a la plantilla del INE.

En la realización de Auditoría participaron activamente 4 Profesores especializados en Desarrollo de Sistemas de Información e Ingeniería de Software, así como 2 especialistas en seguridad informática y 15 alumnos de trimestres avanzados de las licenciaturas en Computación e Ing. Electrónica.

2. Introducción

La auditoría al sistema informático del PREP es una actividad para aumentar la confianza que la ciudadanía pueda tener de él y en los resultados que publique.

La realización de la auditoría implicó gran esfuerzo de los equipos de la UAM-I y del IEEM con un número grande de participantes (21 personas), durante 3 meses calendario.

Este documento presenta el Informe final de la Auditoría al sistema informático del PREP.

El reporte consta de un Resumen ejecutivo describiendo en términos generales las actividades realizadas y los resultados obtenidos.

A continuación de esta introducción se presentan los resultados de cada línea de trabajo de la auditoría.

3. Resultados

3.1. Pruebas Funcionales de Caja Negra

La estrategia de las PFCN consideró 3 ciclos de prueba los cuales fueron reportados en un informe preliminar y en el informe final de esta línea de trabajo.

Se muestran los resultados obtenidos en cada ciclo de pruebas.

3.1.1. Resultados 1er ciclo de prueba

Se hizo la exploración del ambiente de auditoría y se resolvieron todos los problemas de credenciales y configuración de los módulos para que el equipo de la UAM-I pudiera usarlo.

Se hicieron recorridos de prueba no estructurados para explorar el sistema informático.

Se siguió el Proceso Técnico Operativo para verificar que se incorpora en su totalidad en el sistema informático del PREP.

Se diseñaron y se aplicaron cerca de 40 casos de prueba diferentes que cubrieron los módulos de digitalización (PREP Casilla y módulo con digitalización en el CATD), captura, verificación y publicación, de los cuales se obtuvieron hallazgos de prioridad baja que fueron comunicados al personal de IEEM.

luis

3.1.2. Resultados 2º ciclo de prueba

El objetivo de este ciclo fue revisar que los cálculos y aritmética asociada fuera la correcta de acuerdo con las especificaciones electorales, así como validar que los hallazgos reportados del 1er ciclo ya estuviesen resueltos.

Se diseñaron y aplicaron cerca de 40 casos de prueba mismos que generaron observaciones que más adelante fueron aclaradas por el personal del IEEM. Este ciclo no generó hallazgos.

La verificación de corrección de hallazgos del ciclo 1 encontró que todos fueron solventados correctamente.

3.1.3. Resultados 3er ciclo de prueba

Dado que hubo cambios en el sistema informático del PREP después del 2º ciclo, se hizo un 3er ciclo de pruebas para verificar que los cambios no hubiesen generado errores.

Se hizo una prueba de regresión que corresponde a reaplicar los casos de prueba de los ciclos 1 y 2. Este ciclo no generó hallazgos.

3.2. Validación del Sistema Informático del PREP

Esta línea de trabajo plantea asegurar que el sistema informático del PREP en operación el 4 y 5 de junio sea el mismo que fue auditado y por lo mismo todas las conclusiones de la auditoría le son aplicables. Adicionalmente plantea una validación de que no existan actas precargadas antes de que el sistema informático inicie sus operaciones.

Las validaciones tienen que hacerse previo a la operación del PREP, durante la operación del PREP y al cierre de operaciones del PREP, estas validaciones deben hacerse ante un notario público.

Para validar que el sistema informático en operación es el mismo que el que fue auditado, se compara los elementos del sistema informático contra los del sistema auditado. La comparación de elementos se hace mediante la obtención de la firma criptográfica de cada elemento, la cual es única. Si dos elementos son iguales, sus firmas criptográficas son idénticas, si hay una variación por pequeña que sea, las firmas son diferentes.

Las firmas se obtienen mediante un algoritmo que procesa cada byte de un archivo y genera como resultado la firma criptográfica. El algoritmo usado es el SHA-512.

Para poder hacer la validación es necesario desarrollar programas que lean los archivos de los componentes del sistema informático, generen sus firmas criptográficas, hagan lo mismo con el sistema auditado y compare las firmas.

Para validar que no hay actas precargadas, es necesario desarrollar consultas a la base de datos.

Para poder realizar la VSI se elaboró un Procedimiento de Validación que indica la forma en que se harán las distintas actividades de la VSI y se incluyó un Módulo de Validación para poder centralizar los programas de validación.

Se desarrollo un Módulo de Validación que sigue el Procedimiento de Validación y realiza las consultas, generaciones de firmas criptográficas y comparaciones que se requieren.

Este módulo permite visualizar de manera sencilla cada una de las actividades relacionadas con la VSI.

El Procedimiento de Validación se llevará a cabo los días 4 y 5 de junio utilizando el Módulo de Validación.

El resultado de la validación se dará a través de las Constancias de Hechos para los siguientes puntos del Proceso de Validación:

- Toma de huellas criptográficas del ambiente de auditoría
- Validación del sistema informático previo al inicio de operaciones del PREP.
- Validación del sistema informático durante la operación del PREP.
- Validación del sistema informático al cierre de la operación del PREP.

El módulo de validación consulta al ambiente de operación del PREP, para cumplir con las normativas de seguridad, se ejecuta desde una computadora asignada por el personal del IEEM.

3.3. Análisis de Vulnerabilidades

Se realizó un análisis del sistema informático del PREP para detectar puntos de debilidad que puedan ser aprovechados por atacantes.

Se aplicaron herramientas automáticas de reconocimiento de vulnerabilidades y se analizaron los datos correspondientes. De este análisis se encontraron hallazgos que fueron reportados al equipo del IEEM, que fueron resueltos. Posteriormente se rehicieron algunos

análisis para asegurar que los hallazgos estuviesen resueltos. Todos los hallazgos tuvieron un nivel bajo de gravedad y no pusieron en riesgo al sistema informático.

Como parte del análisis de vulnerabilidades, se realizó la revisión a las configuraciones de todos los elementos del sistema informático del PREP y de su infraestructura tecnológica para asegurar que son las adecuadas en términos de seguridad de acuerdo con las mejores prácticas en esta materia.

Se revisaron las configuraciones de cada componente del sistema informático contra las recomendaciones de las mejores prácticas. De esta revisión se encontraron hallazgos que fueron corregidos por el equipo del IEEM y validada su solución por el equipo de la UAM-I. Los hallazgos fueron de nivel bajo de severidad y no ponían en riesgo al sistema informático.

La parte final del análisis de vulnerabilidades fue la aplicación de pruebas intentando pasar las defensas del sistema informático considerando la información recabada en las 2 primeras sublíneas de trabajo.

Se realizaron estas pruebas de las cuales surgieron hallazgos de bajo nivel de gravedad, los cuales fueron notificados al equipo del IEEM para su tratamiento. Posteriormente el equipo de la UAM-I valido su solución. Todos los hallazgos encontrados fueron resueltos y ninguno puso en riesgo la seguridad del sistema informático.

3.4. Análisis de Código Fuente

Se realizó el análisis del código fuente de todos los componentes del sistema informático del PREP mediante la ejecución de herramientas especializadas que señalan elementos de riesgo dentro de la programación de acuerdo con las mejores prácticas de programación segura.

Al equipo de la UAM-I le fue proporcionado el código fuente de todos los componentes desarrollados para sistema informático del PREP. El equipo UAM-I uso varias herramientas especializadas para hacer el análisis de ese código fuente. De los resultados, el equipo de la UAM-I hizo un análisis para filtrar los hallazgos que realmente fueran significativos. Estos hallazgos fueron notificados al equipo del IEEM para su resolución y posteriormente el equipo de la UAM-I valido su correcta solución.

Todos los hallazgos encontrados fueron resueltos y ninguno puso en riesgo la seguridad del sistema informático.

3.5. Pruebas de Negación de Servicio

Se realizaron pruebas de negación de servicio que consisten en enviar tráfico que simule un ataque a los sitios de publicación de resultados y al del IEEM.

Los sitios a los que se les aplicaron las pruebas son:

- Sitio principal del IEEM hhtp://www.ieem.org.mx
- Sitio de publicación de resultados del PREP http://prep.ieem.mx

Las pruebas aplicadas consideraron protocolos de capa 4 y capa 7

La prueba se realizó de acuerdo con la especificación del anexo técnico, mediante el uso de una plataforma proporcionada por un tercero autorizado.

3.5.1. Resultados 1er ciclo de pruebas

Se aplico la prueba de acuerdo con la especificación del anexo técnico a los sitios especificados. Esta prueba fue realizada por el personal de la UAM-I y en presencia de personal del IEEM.

Se encontró un hallazgo para el sitio del IEEM.

El personal del IEEM comunicó que atendería el hallazgo y se programó un 2º ciclo de prueba para validar la corrección realizada por el personal del IEEM.

3.5.2. Resultados 2º ciclo de pruebas

Se aplico la prueba de acuerdo con la especificación del anexo técnico solo al sitio afectado. Esta prueba fue realizada por el personal de la UAM-I y en presencia de personal del IEEM.

Se encontró que el hallazgo permaneció.

El personal del IEEM comunicó que atendería de otra manera el hallazgo y se programó un 3er ciclo de prueba para validar la corrección realizada por el personal del IEEM.

3.5.1. Resultados 3er ciclo de pruebas

Se aplico la prueba de acuerdo con la especificación del anexo técnico solo al sitio afectado. Esta prueba fue realizada por el personal de la UAM-I y en presencia de personal del IEEM.

Se encontró que el hallazgo permaneció.

El personal del IEEM comunicó que atendería de otra manera distinta el hallazgo y se programó un 4° ciclo de prueba para validar la corrección realizada por el personal del IEEM.

3.5.1. Resultados 4° ciclo de pruebas

Se aplico la prueba de acuerdo con la especificación del anexo técnico solo al sitio afectado. Esta prueba fue realizada por el personal de la UAM-I y en presencia de personal del IEEM.

Se encontró que el hallazgo fue resuelto satisfactoriamente, pues se aplicaron en su totalidad todas las pruebas especificadas y los resultados fueron satisfactorios.

3.6. Revisión del Apego del Sitio de Publicación

Esta revisión se realizó junto con los ciclos de las Pruebas Funcionales de Caja Negra y se aplicó a la versión de escritorio y a la versión para dispositivo móvi.

En el primer ciclo se identificaron las plantillas del INE y se identificaron los elementos en el sitio de publicación de resultados.

Se hicieron revisiones preliminares y se encontraron hallazgos menores, los cuales fueron reportados al personal del IEEM.

El segundo ciclo fue más estructurado y se validó la corrección de los hallazgos del 1er ciclo.

Este segundo ciclo genero hallazgos menores, los cuales fueron reportados al personal de IEEM. Estos hallazgos fueron atendidos durante la aplicación de este segundo ciclo.

Dado que el sistema del PREP tuvo actualizaciones, se realizó un 3er ciclo de revisión y no se encontraron hallazgos de apego a la plantilla proporcionada por el INE.

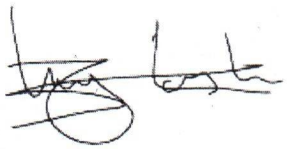
Es importante señalar que todos hallazgos detectados no ponían en riesgo la publicación de los resultados.

4. Conclusiones

Después de realizar todas las actividades planteadas en el Anexo Técnico, la auditoría al sistema informático del PREP emite las siguientes conclusiones:

- El sistema informático del PREP realiza las funciones de su especificación y las que le marca el Proceso Técnico Operativo.
- El sistema informático del PREP no tiene vulnerabilidades de seguridad significativas que pongan en riesgo su operación.
- El código que conforma al sistema informático del PREP sigue las buenas prácticas de codificación segura.
- El sitio de publicación de resultados del PREP y el sitio institucional del IEEM pueden resistir ataques de negación de servicio como los especificados en el Anexo Técnico.
- El sitio de publicación de resultados del PREP en su versión de escritorio y en su versión de dispositivo móvil, se apegan a las plantillas proporcionadas por el INE.

Adicionalmente, se cuenta con un mecanismo que valida que el sistema informático del PREP el día de la elección es idéntico al sistema informático que fue utilizado durante la auditoría y por lo mismo las afirmaciones hechas por la auditoría le son aplicables.



Ing. Luis Fernando Castro Careaga
Responsable del Proyecto de Auditoría
al sistema informático del PREP