Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA
Unidad Iztapalapa

Auditoría al sistema informático e infraestructura tecnológica del PREP del Proceso Electoral Ordinario 2021-2022 en el Estado de Oaxaca

Informe Final

---

03 de junio de 2022

Aprobación del Documento

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

03 de junio de 2022

Historia de Cambios

Fecha	Versión	Autor	Descripción
2/06/2022	0.1	ERF, OLCJ, LTF, JMCV, RMR y LFCC	Versión inicial
03/06/2022	1.0	LFCC	Versión final revisada

Contenido

1 Resumen ejecutivo

El 9 de marzo del 2022, la UAM-I y el IEEPCO firmaron un convenio de colaboración para la Auditoría al sistema informático e infraestructura tecnológica del PREP del Proceso Electoral Ordinario 2021-2022 en el Estado de Oaxaca 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 4 líneas de trabajo.

Pruebas funcionales de caja negra al sistema informático del PREP (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, sin tomar en cuenta la forma en que está construido.

Se realizaron 3 ciclos de prueba aplicándose pruebas manuales para asegurar que el sistema funciona como se espera. Los hallazgos encontrados por el equipo de la UAM-I fueron notificados al equipo del IEEPCO, el cual los atendió y el equipo de la UAM-I verifico su correcta resolución.

De los resultados de las PFCN puede afirmarse que el sistema informático funciona como se espera y no tiene funciones que no estén dentro de sus especificaciones.

Validación del sistema informático y de sus base de datos

Esta validación tiene como objetivo asegurar que el sistema informático usado para el PREP 2022 es el mismo que fue auditado, así como asegurar que al iniciar la operación del PREP 2022, este inicializado correctamente y no existan actas precargadas.

Para hacer la validación se elaboraron procedimientos para extraer las firmas electrónicas de los componentes y hacer consultas a las bases de datos del PREP 2022 lo cual permite hacer las validaciones previo al inicio de operaciones, durante la operación y al cierre de operaciones del PREP 2022.

Estos procedimientos serán utilizados los días de 5 y 6 de junio para las actividades de validación.

Análisis de vulnerabilidades a la infraestructura tecnológica y servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP

Esta línea de trabajo tiene como objetivo asegurar que el sistema informático del PREP 2022 está construido de manera segura y es resistente a ataques.

Se realizaron análisis de vulnerabilidades, se hicieron pruebas de penetración y se revisaron las configuraciones del sistema informático del PREP y su infraestructura tecnológica, se hicieron pruebas de penetración, tanto en infraestructura basada en la *nube* como en la evaluación de un CATD.

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

De los resultados de la APSI se puede afirmar que el sistema informático del PREP 2022 es seguro y es capaz de resistir ataques informáticos.

Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal de "EL IEEPCO"

Esta línea de trabajo tiene como objetivo realizar ataques que envían gran volumen de peticiones a los servidores para intentar saturarlos que permitan identificar, evaluar y aplicar las medidas necesarias para asegurar la correcta y continua disponibilidad del servicio Web, así como de los sitios de publicación de resultados del PREP y del sitio principal de "EL IEEPCO", durante el periodo de operación del PREP.

Se realizaron las pruebas de acuerdo con las especificaciones indicadas en el Anexo Técnico del Convenio de Colaboración y se comprobó que los mecanismos de protección del PREP 2022 funcionaron de manera adecuada.

De los resultados de estas pruebas se puede afirmar que el sistema informático del PREP 2022 es capaz de resistir ataques de saturación.

En la realización de Auditoría participaron activamente 5 Profesores especializados en Desarrollo de Sistemas de Información e Ingeniería de Software, así como 3 especialistas en seguridad informática y 10 alumnos de trimestres avanzados de las licenciaturas en Computación e Ing. Electrónica.

2 Introducción

La auditoría al sistema informático del PREP 2022 es una actividad para aumentar la confianza en él y en los resultados que publique.

La realización de la auditoría implicó gran esfuerzo de los equipos de la UAM-I y del IEEPCO con un número grande de participantes (cerca de 40 personas), casi 3 meses calendario.

Este documento presenta el Informe final de la Auditoría al sistema informático del PREP 2022.

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 Resultados de las Pruebas Funcionales de Caja Negra al sistema informático del PREP

La metodología utilizada se basó en el seguimiento del flujo que debe seguir la información de acuerdo con las descripciones asentadas en los documentos de requerimientos.

Se efectuó la ejecución del flujo de información del sistema siguiendo las trayectorias primarias o correctas (*happy path*) y dejando al final los caminos alternos que en este sistema están considerados en el tratamiento de incidencias.

Para realizar las pruebas, se siguió el flujo natural de la información considerando tanto escenarios correctos como escenarios incorrectos en la dirección del flujo. Las pruebas se dividieron en 4 líneas:

1. Se realizaron los procesos de Digitalización, Captura y Publicación con énfasis en:
   - La verificación de que los Cálculos publicados sean correctos y
   - La verificación de que la Base de Datos que se descargó de la página del PREP no contenía actas al inicio del proceso.

   Estas pruebas se realizaron durante los días 25 y 26 de abril del 2022.
2. Se realizaron los procesos de Digitalización, Captura y Publicación con énfasis en:
   - La validación de los campos en tipo de dato y longitud del dato.

   Esta prueba se realizó el día 26 de abril del 2022.
3. Se verificó el apego de la consulta del PREP a las plantillas proporcionadas por el INE y a las Normas Aplicables en:
   - Pantalla completa en aplicación de escritorio y

- Aplicación móvil.

Estas pruebas se realizaron el día 27 de abril del 2022.

4. Se realizaron los procesos de Digitalización, Captura y Presentación con énfasis en:
   - Manejo de actas con incidencias y
   - Voto en el extranjero.

   Estas pruebas se realizaron el día 30 de abril del 2022.

En estas líneas se detectaron incidencias que fueron comunicadas al IEEPCO y al proveedor del Sistema PREP para su atención.

Las incidencias detectadas fueron de severidad baja y en ningún momento ponen en riesgo de errores en los resultados que genere el sistema del PREP.

En reunión con personal del proveedor se realizó la revisión de los hallazgos haciendo las aclaraciones correspondientes y registrando que las observaciones ya fueron atendidas.

Es por lo que se considera que el Sistema PREP 2022 cumple con los requerimientos funcionales y los resultados que genere serán el reflejo fiel de las actas que se registren.

3.2 Resultados de la Validación del Sistema Informático y de sus bases de datos

Esta línea de trabajo plantea asegurar que el sistema informático del PREP en operación el 5 y 6 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 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.

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

Para validar que no hay actas precargadas, es necesario incorporar consultas a las bases de datos en los procedimientos ya mencionados.

Para poder realizar la validación se elaboró un Procedimiento de Validación que indica la forma en que se harán las distintas actividades de la VSIBD. Este procedimiento fue probado en los simulacros del PREP llevados a cabo los días 15, 22 y 29 de mayo, lo cual permitió hacer ajustes para una mejora ejecución durante el proceso de validación.

El Proceso de Validación se llevará a cabo los días 5 y 6 de junio utilizando procedimiento 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 2022.
- Validación del sistema informático durante la operación del PREP 2022.
- Validación del sistema informático al cierre de la operación del PREP 2022.

3.3 Resultados del Análisis de vulnerabilidades a la infraestructura tecnológica y servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP

El objetivo de esta línea de trabajo es asegurar que el sistema informático del PREP 2022 que está construido de manera segura y es resistente a ataques.

Esta línea de trabajo a su vez constituida por 3 sublíneas:

- **Análisis de vulnerabilidades**

  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 hicieron hallazgos que fueron reportados al equipo del IEEPCO, los cuales fueron resueltos. Posteriormente se rehicieron algunos análisis para asegurar que los hallazgos se hubieran resuelto. Todos los hallazgos tuvieron un nivel bajo de gravedad y no pusieron en riesgo al sistema informático.

- **Revisión de configuraciones**

  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 hicieron

hallazgos que fueron corregidos por el equipo del IEEPCO y validada su solución por el equipo de la UAM-I. Los hallazgos fueron de nivel bajo de gravedad y no ponían en riesgo al sistema informático.

- **Pruebas de penetración**

  Consiste en 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 se hicieron hallazgos de bajo nivel de gravedad, los cuales fueron notificados al equipo del IEEPCO 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 Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal de "EL IEEPCO"

Las actividades de esta línea de trabajo se realizaron en el período del 12 de mayo de 2022 al 27 de mayo de 2022.

Se realizaron las pruebas de acuerdo con las especificaciones indicadas en el Anexo Técnico del Convenio de Colaboración y se comprobó que los mecanismos de protección del PREP 2022 funcionaron de manera adecuada.

Las pruebas se aplicaron al portal principal del IEEPCO, al portal de publicación de resultados y al sitio principal de recepción de actas digitales del PREP. Las pruebas realizadas no identificaron hallazgos.

Las pruebas realizadas no generaron evidencia de vulnerabilidades, por el contrario, mostraron que los mecanismos de defensa de la infraestructura se comportan como es esperado. En conclusión, la infraestructura es capaz de resistir ataques con las características de las pruebas realizadas.