Auditoría al sistema informático y a la infraestructura tecnológica del Programa de Resultados Electorales Preliminares 2021

Informe Final

4 de junio de 2021

Aprobación del Documento

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

4 de junio de 2021

Historia de Cambios

Fecha	Versión	Autor	Descripción
4/6/2021	1.0	LFCC OLCJ JMCV HCM	Versión final

Tabla de Contenido

1. Resumen ejecutivo

El 30 de noviembre del 2020, la UAM-I y el INE firmaron un convenio de colaboración para la Auditoría al sistema informático y a la infraestructura tecnológica del Programa de Resultados Electorales Preliminares 2021 teniendo como objetivo final validar ante la sociedad que el sistema informático del PREP 2021 es confiable y seguro.

La auditoría se realizó a través de 3 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, sin tomar en cuenta la forma en que está construido.
>
> Se realizaron 5 ciclos de prueba aplicándose pruebas manuales y pruebas automatizadas para asegurar que el sistema funciona como se espera. Los hallazgos encontrados por el equipo de la UAM-I fueron notificados al equipo del INE, el cuál 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 del PREP 2021 funciona como se espera y no tiene funciones que no estén dentro de sus especificaciones.

Auditoría y pruebas de seguridad informática (APSI)

> La APSI tiene como objetivo asegurar que el sistema informático del PREP 2021 que está construido de manera segura y es resistente a ataques.
>
> Se realizaron análisis de vulnerabilidades, se revisaron las configuraciones se analizó el código fuente de los programas del PREP 2021, se hicieron pruebas de penetración y pruebas de ataques masivos (pruebas DDoS).
>
> Los hallazgos encontrados por el equipo de la UAM-I fueron notificados al equipo del INE, el cuál 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 2021 es seguro y es capaz de resistir ataques informáticos.

Validación del sistema informático y de su base de datos (VSIBD)

> La VSIBD tiene como objetivo asegurar que el sistema informático usado para el PREP 2021 es el mismo que fue auditado, así como asegurar que al iniciar la operación del PREP 2021, este inicializado correctamente y no existan actas precargadas.
>
> Para hacer la validación se desarrollo un módulo de validación que permite hacer las validaciones previo al inicio de operaciones, durante la operación y al cierre de operaciones del PREP 2021.
>
> Este módulo será utilizado los días de 6 y 7 de junio para las actividades de la VSIBD.

En la realización de Auditoría participaron activamente 4 Profesores especializados en Desarrollo de Sistemas de Información e Ingeniería de Software, así como 6 especialistas en seguridad informática y 24 alumnos de trimestres avanzados de las licenciaturas en Computación e Ing. Electrónica.

2. Introducción

La auditoría al sistema informático del PREP 2021 es una actividad para aumentar la confianza en el PREP 2021 y los resultados que publique.

La realización de la auditoría implicó gran esfuerzo de los equipos de la UAM-I y del INE con un número grande de participantes (cerca de 40 personas), durante 5 meses calendario.

Este documento presenta el Informe final de la Auditoría al sistema informático del PREP 2021.

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

La estrategia de las PFCN consideró 5 ciclos de prueba los cuales fueron reportados en los dos informes preliminares de esta línea de trabajo.

Se muestran los resultados obtenidos en cada ciclo de pruebas.

3.1.1. Resultados 1er ciclo de pruebas

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.

En el 1er ciclo de PFCN se consideró revisar la factibilidad de las pruebas automatizadas.

El enfoque de pruebas automática sobre interfaces de usuario que residen en navegadores de internet requiere la identificación de los distintos objetos que componen la página visualizada, para sobre ellos hacer las lecturas y/o escrituras de información por parte del autómata de prueba.

Los objetivos de las Pruebas Automáticas para el 1er ciclo de pruebas fueron:

- Reconocer la interfaz en el navegador de internet de los módulos de PREP 2021.
- Desarrollar el código para un caso de prueba automática sobre el diálogo de Autenticación de cualquier módulo del PREP 2021.

Ya con el ambiente de auditoria del PREP 2021, se reconoció la interfaz y se vio que es factible la utilización del enfoque de prueba automática, pues se tienen todos los elementos necesarios en la información del diálogo.

Después de este reconocimiento, se procedió a desarrollar un prototipo para el autómata de prueba para el diálogo de acceso al sistema.

El caso de prueba a considerar es con respecto a una autenticación exitosa y varias situaciones de autenticación no exitosa.

Para instrumentar los escenarios de pruebas de autenticación no exitosa, se consideraron casos como caracteres inválidos y cadenas de tamaño muy grande.

El autómata fue desarrollado y ejecutado dando como resultado que las pruebas diseñadas se cumplieron correctamente en el acceso de los módulos del sistema informático.

3.1.2. Resultados 2º ciclo de pruebas

Se realizó un ejercicio de prueba manuales para recorrer todos los módulos del sistema informático usando 523 actas. Las actas fueron llenadas por el equipo de la UAM-I y se siguió todo el proceso operativo, desde colocar la fecha y hora a cada acta, colocar las etiquetas con la identificación de la casilla, capturar su imagen por todos los medios que

permite el procedimiento operativo, para continuar con la capturas de sus datos, su cotejo y finalmente la publicación de los resultados.

Se generaron hallazgos que fueron notificados al equipo del INE, que una vez corregidos se revisaron en el 3er ciclo de prueba.

En términos de pruebas automatizadas las acciones y resultados se describen a continuación

El enfoque de pruebas automáticas depende de conocer el estado que guarda la interfaz con el usuario. Dado que los módulos del PREP tratan con imágenes de las actas, es necesario identificar las imágenes para poder aplicar datos específicos para la ejecución del caso de prueba.

Los objetivos de las Pruebas Automáticas para el 2º ciclo de pruebas son:

- Encontrar mecanismos para la identificación de las imágenes en los módulos, para poder referenciar a los datos de prueba.
- Generar un prototipo que pueda manejar los tres tipos de actas y que permita la captura de datos de las actas.

Para lograr el 1er objetivo se analizó la pantalla en la que presentan las imágenes de un acta a capturar. En el navegador es posible identificar de manera única y consistente las imágenes a través de su contenido binario. A este contenido binario se le aplica una función de hash para poder obtener un identificador único que pueda manejarse en un programa. Ese identificador será utilizado para referenciar a los datos a capturar en el caso de prueba para esa acta.

Se hizo la programación correspondiente y ya obtuvo el identificador, eso implica que hay que hacer dos recorridos de los flujos operativos del PREP, el primero para registrar los identificadores y el segundo sería la aplicación de los casos de prueba automáticos.

Una vez con el identificador, se pueden llenar los campos con valores predeterminados que serían los valores que se tienen para el acta en cuestión.

Con respecto al prototipo, solo se generaron valores sin ninguna lógica y/o relación para registrar el acta.

3.1.3. Resultados 3er ciclo de pruebas

Se hicieron 2 ejercicios de pruebas manuales para corroborar los hallazgos del 2º ciclo y corroborar que se han corregido los que el equipo del INE resolvió.

Esos ejercicios fueron realizados con un número menor de actas.

Los resultados de estos ejercicios comprobaron que algunos hallazgos ya estaban resueltos y también se encontró que algunos otros todavía prevalecían.

Con respecto a las pruebas automáticas, una vez que los mecanismos para llevar a cabo la prueba automática han sido explorados, es necesario la creación de los autómatas para cada módulo del Sistema Informático.

Los objetivos de las Pruebas Automáticas para el 3er ciclo de pruebas fueron:

- Desarrollar una primera versión de recorrido de prueba automática para cada módulo del Sistema Informático.
- Estudiar las estrategias de aplicación de los escenarios de prueba automática.

Se desarrollaron y probaron tres autómatas uno por cada etapa del proceso operativo del PREP.

Con respecto a las posibles estrategias de aplicación de escenarios, se identificó que pueden existir en operación varios autómatas de manera simultánea para cada módulo, teniendo una simulación muy parecida a la realidad de una prueba manual con varios testers.

Al finalizar esta etapa se identificaron algunas acciones adicionales para revisar con los autómatas como son el registro en las bitácoras de cada paso que el autómata realice.

3.1.4. Resultados 4º ciclo de pruebas

Todos los ejercicios se realizaron utilizando pruebas automatizadas.

Se tuvieron 15 sesiones de prueba ejecutando 50 flujos de prueba en cada una dando un total de 750 flujos totales de casos de prueba durante el ciclo.

La situación más recurrente en los ejercicios surgió con un mensaje de error “Acta fuera de Catálogo”. Las actas fuera de catálogo son actas que estuvieron activas en los ciclos de prueba 2 y 3, pero que el equipo del INE al actualizar la información relacionada con las casillas que se abrirán el 6 de junio elimino de la base de datos de actas a ser procesadas por el PREP, por lo mismo el sistema informático del PREP marcaba el error “Acta fuera de catálogo” en esos casos. Esas actas se eliminaron de los flujos de los casos de prueba.

Los resultados de estos ejercicios comprobaron que algunos hallazgos ya estaban resueltos y también se encontró que algunos otros todavía prevalecían, mismos que fueron considerados para el quinto ciclo de pruebas.

3.1.5. Resultados 5º ciclo de pruebas

Este ciclo de pruebas estuvo caracterizado por la realización de las pruebas sobre el ambiente de auditoría actualizado para que fuera idéntico al ambiente de operación del PREP 2021 para los días 6 y 7 de junio. Además de utilizar los formatos finales para las actas a procesar.

La primera parte del mes se dedico a registrar las firmas criptográficas del nuevo conjunto de actas a ser utilizadas.

Se tuvieron 8 sesiones de prueba ejecutando 27 flujos de prueba en cada una dando un total de 216 flujos totales de casos de prueba durante el ciclo.

El ambiente de auditoría para ejecutar pruebas caja negra no estuvo disponible en dos periodos: del 3 al 7 de mayo y del 24 al 30 de mayo.

Además, se tuvieron sesiones para ajustar los accesos y credenciales del equipo para poder ejecutar las pruebas. Los resultados de estos ejercicios comprobaron que todos los hallazgos ya fueron resueltos.

3.2. Resultados de la Auditoría y Pruebas de Seguridad Informática

La APSI tiene como objetivo asegurar que el sistema informático del PREP 2021 que está construido de manera segura y es resistente a ataques.

Esta línea de trabajo a su vez constituida por 5 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 encontraron hallazgos que fueron reportados al equipo del INE, que los resolvieron. Posteriormente se rehicieron algunos análisis para asegurar la solución de los hallazgos. 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 encontraron hallazgos que fueron corregidos por el equipo del INE 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.

- **Análisis de código fuente en materia de seguridad**

  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 INE para su resolución y posteriormente el equipo de la UAM-I valido su correcta solución.

- **Pruebas de penetración**

  Aplicación de pruebas intentando pasar las defensas del sistema informático considerando la información recabada en las 3 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 INE 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.

- **Pruebas de ataques masivos (pruebas DDoS)**

  Aplicación de pruebas de tráfico masivo para validar que tan resilente el sistema informático ante este tipo de ataques.

  Se realizaron estas pruebas en conjunto con el equipo del INE y el sistema informático y su infraestructura tecnológica resistieron perfectamente dichos ataques, validando que son capaces de resistir este tipo de ataques.

Evaluación de seguridad a un Centro de Acopio, Captura y Digitalización (CATD).

Se realizó la visita a un CATD para asegurar que su infraestructura fuera segura. Se ejecutaron análisis de vulnerabilidades, revisión de configuraciones y pruebas de penetración. Los hallazgos detectados fueron de bajo nivel de gravedad y fueron enterados al equipo del INE.

De los resultados de la APSI se puede afirmar que el sistema informático del PREP 2021 es seguro y es capaz de resistir ataques informáticos como los practicados durante la auditoría.

3.3. Resultados de la Validación del Sistema Informático y de su base de datos

Esta línea de trabajo plantea asegurar que el sistema informático del PREP en operación el 6 y 7 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. El algoritmo usado es el SHA-256.

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 programas que consulten la base de datos.

Para poder realizar la VSIBD se elaboró un Procedimiento de Validación que indica la forma en que se harán las distintas actividades de la VSIBD 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 VSIBD.

El Procedimiento de Validación se llevará a cabo los días 6 y 7 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 2021.
- Validación del sistema informático durante la operación del PREP 2021.
- Validación del sistema informático al cierre de la operación del PREP 2021.

El módulo de validación consulta al ambiente de operación del PREP, para cumplir con las normativas de seguridad, se tuvo que configurar de manera especial la computadora en la que se ejecutará el Módulo de Validación.