

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



**Auditoría Informática al Sistema Electrónico
por Internet (SEI) para el IECM**

**Informe de Evaluación de la Auditoría Informática
(informe posterior a la jornada)**

**Periodo de evaluación:
Del 15 al 17 de marzo de 2020**

Handwritten signature and initials.

Bitácora de modificaciones

Historial de versiones

Versión	Fecha	Descripción del cambio	Autor
0.0.1	17/03/2020	Creación del documento	Marcelo Pérez Medel
0.1.0	17/03/2020	Redacción inicial	Paulett Toledo Varela
0.2.0	17/03/2020	Revisión del documento	Diego Rocha Zamudio
0.3.0	18/03/2020	Modificaciones	Axel Jesús Pantoja Romo
0.3.1	18/03/2020	Redacción de resultados	Paulett Toledo Varela
1.0.1	18/03/2020	Revisión general	Jesús Hernández Cabrera
1.1.0	27/03/2020	Revisión final	Marcelo Pérez Medel
1.1.1	27/03/2020	Revisión ortografía, redacción y errores de captura (dedazos)	César Fonseca Guízar

Contenido

1.	OBJETIVO GENERAL.....	1
2.	OBJETIVOS ESPECÍFICOS.....	1
3.	ALCANCES.....	3
4.	RESULTADOS DE LA AUDITORÍA.....	4
5.	CONCLUSIONES.....	7
6.	RECOMENDACIONES.....	8

1. OBJETIVO GENERAL

Realizar una auditoría informática al Sistema Electrónico por Internet (SEI), del Instituto Electoral de la Ciudad de México conforme a los Lineamientos Generales del Sistema Electrónico por Internet "SEI". Mismos que fueron aprobados el 16 de noviembre de 2019 por el Consejo General mediante acuerdo IECM/ACU-CG-077/2019.

2. OBJETIVOS ESPECÍFICOS

- A. Revisar el sistema informático y los correspondientes aplicativos desarrollados específicamente para el SEI en términos de funcionalidad. La auditoría deberá determinar, mediante un análisis detallado del código, que los aplicativos SEI realizan las funciones descritas en el manual de usuario y solamente esas, es decir, el programa solamente hace lo que se espera de él, procesando transparente y correctamente la información desde su origen hasta la publicación.

Dentro de los aspectos a revisar en el rubro de calidad del sistema se incluyen:

- Verificación de la arquitectura del sistema.
- Controles adecuados en la entrada de datos.
- Almacenamiento y restauración de datos.
- Implementación de bitácoras en el procesamiento de datos sensibles.
- Cumplimiento en buenas prácticas de codificación basado en estándares en donde se protejan los componentes por medio de encapsulamiento, niveles de acceso y buena implementación de estructuras de control.
- Manejo de errores.
- Evaluación de desempeño y ausencia de leaks de memoria y recursos.

- B. Probar todos los aplicativos desarrollados específicamente para el SEI en términos de funcionalidad.
- C. Analizar las posibles vulnerabilidades de la infraestructura tecnológica del SEI.
- 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 SEI.

3. ALCANCES

- A. La auditoría se realizó del 24 de febrero al 16 de marzo de 2020.
- B. La auditoría consiste en dos partes: La primera, corresponde a revisión de la funcionalidad e inspección de código fuente; la segunda, identifica posibles vulnerabilidades que tenga el sistema.
- C. Se realizó una planificación de la auditoría, identificando claramente los recursos materiales y técnicos necesarios para llevarla a cabo; dicha planificación se encuentra en poder de la Unidad Técnica de Servicios Informáticos.
- D. La auditoría se realizó con base a los requerimientos establecidos en el anexo técnico del convenio de colaboración UNAM – IECM y en la metodología IEEE Std 1028™-2008 "IEEE Standard for Software Reviews and Audits" la cual es una metodología estandarizada internacionalmente.

4. RESULTADOS DE LA AUDITORÍA

Durante la realización de la auditoría, el equipo auditor se abstuvo de:

- Instalar cualquier tipo de puerta trasera o aplicación que permita acceso remoto encubierto y reiterado.
- Instalar cualquier tipo de keylogger, boot, troyano, rootkit o tecnología similar.
- Instalar aplicaciones de acceso remoto que sean claramente identificables como procesos activos y cuyos puertos, y conexiones sean visibles.
- Borrar, alterar o apagar el uso de las bitácoras (logs) en cualquier dispositivo, estación de trabajo o servidor.
- Modificar la configuración de un servidor, estación de trabajo o dispositivo de red.

Una vez concluida la auditoría, el equipo auditor no dejó ninguna modificación o rastro en la infraestructura del IECM originado a raíz de las pruebas realizadas.

Durante nuestra participación en la auditoría aparte de realizar todas las revisiones y pruebas que se presentan en las siguientes secciones, visitamos distritos electorales para realizar revisiones y tuvimos presencia en el Instituto durante todos los simulacros y los monitoreamos tanto en sitio como desde fuera.

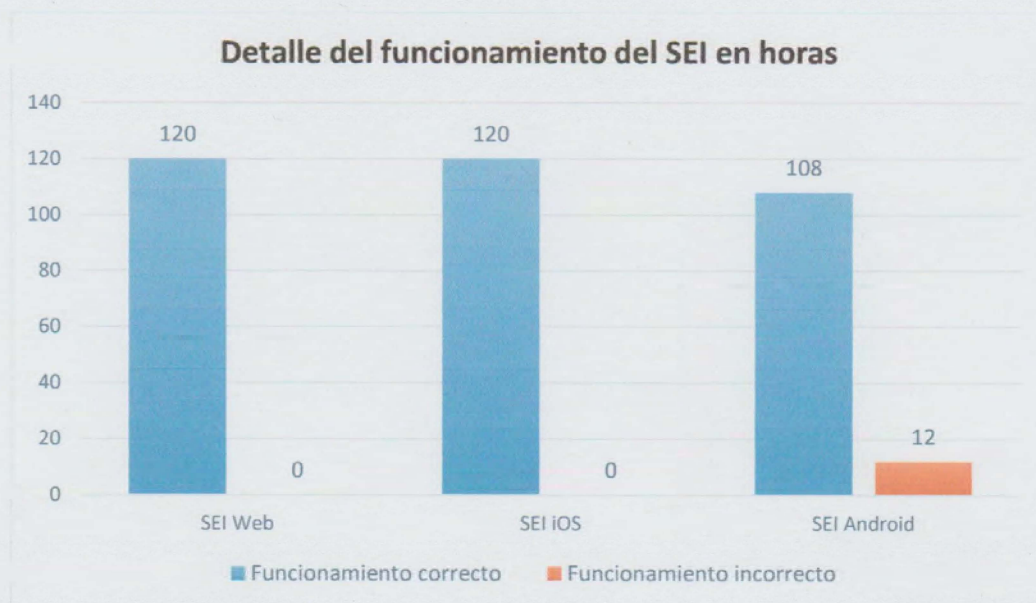
Ejecución de la revisión

Durante las revisiones se pudo corroborar que se implementaron las funcionalidades necesarias, suficiente para la operación del sistema durante la jornada. Se concluyó que el sistema hace lo que debe hacer y nada más.

Respecto a la revisión de seguridad del sistema, no se encontraron vulnerabilidades ni hallazgos críticos que afectaran la ejecución del sistema, además, se sugirió revisar todos los hallazgos no críticos para su posterior mitigación o aceptación. También se concluyó que la infraestructura del SEI es aceptable.

Resultados de la jornada del 8 al 12 de marzo (SEI remoto)

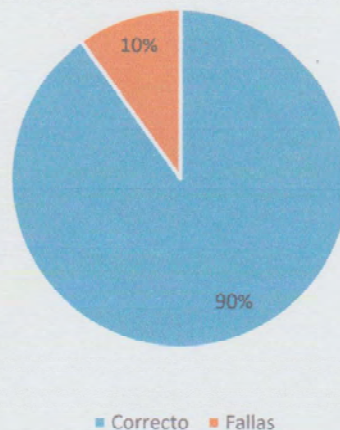
Durante la jornada del 8 al 12 de marzo, el SEI se puso en marcha en tres modalidades, web y en aplicaciones para iOS y Android. El sistema funcionó correctamente en las dos primeras, sin embargo, se registró un mal funcionamiento en la aplicación para Android durante las primeras doce horas, el IECM realizó las correcciones pertinentes y el resto de la jornada el sistema funcionó de manera correcta.



Con base a esto, de las 120 horas de funcionamiento del SEI, la aplicación para Android presentó fallas durante el 10% de la jornada, lo cual es un problema de disponibilidad.

El problema se debió a que mientras en iOS el cambio del escenario de los simulacros al escenario real se realizó de forma transparente en Android se presentó un problema con el manejo de las boletas, lo cual se resolvió realizando unos ajustes en el código. Es importante mencionar que el sentido de los votos no se vio comprometido.

Tiempo de funcionamiento SEI Android



Resultados de la jornada del 15 de marzo (SEI en mesas receptoras)

El día 15 de marzo del presente inició la operación del Sistema Electrónico por Internet (SEI) a las 9:00 hrs, prácticamente desde ese momento se comenzaron a recibir llamadas reportando problemas, los cuales eran principalmente:

- Poca o nula señal para conectarse vía Internet
- Error de conexión de las iPads con el SEI

El segundo resultó ser el error más crítico, ya que se presentó en prácticamente en todas las terminales, cabe mencionar que para ese momento se empezó a notar un cuello de botella en los servidores y si bien algunas terminales lograron establecer conexión poco después la perdían.

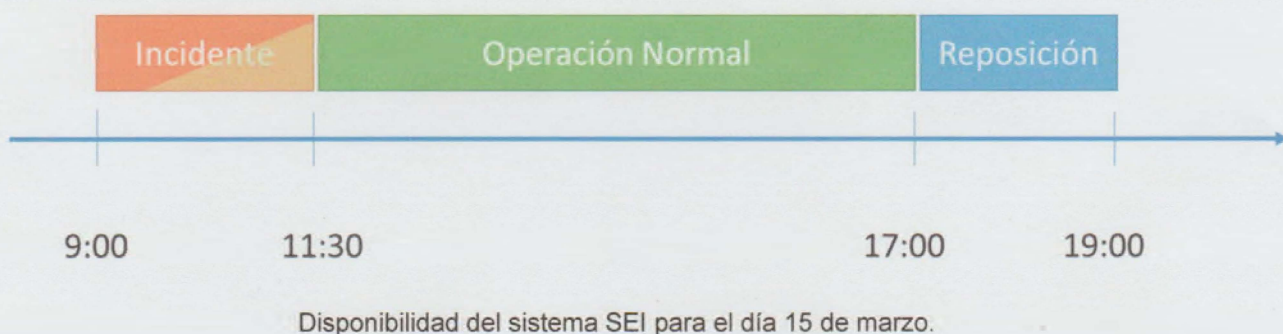
Debido a los siguientes hechos la respuesta por parte de la mesa de ayuda fue:

- Corroborar que el dispositivo contara con una buena señal para su correcto funcionamiento.
- Reiniciar del dispositivo.

- Revisar que se estuviera ingresando de manera correcta la información para acceder a la aplicación.
- Solicitar la espera de 10 minutos antes de volver a reintentar.

Se realizaron varias pruebas para paliar el problema y poco después de las 11:30 am se logró mitigar el cuello de botella gracias a modificaciones en la configuración del número de reintentos y limitar el tiempo máximo de las conexiones. Para este momento cerca de la mitad de las mesas se habían decidido por cambiar de la modalidad electrónica a papel.

La disponibilidad del sistema presentó fallas por 2.5 horas, tiempo en el que sólo se tenía acceso de forma intermitente por breves instantes, por lo que se decidió ampliar la jornada por dos horas, esto se puede apreciar en la siguiente gráfica:



Como parte de la auditoría se realizó un análisis forense para verificar las causas del incidente, las cuales fueron informadas al IECM para que las tome en consideración para el futuro.

5. CONCLUSIONES

- Durante la mayor parte de la jornada el SEI funcionó correctamente y el sentido de los votos no se vio comprometido.
- La disponibilidad del sistema no fue la esperada tanto en la versión remota como en la aplicación iPad, en nuestra opinión se debió a que las pruebas realizadas

durante los simulacros no fueron lo suficientemente cercanas a las condiciones reales de la jornada.

- Después de la revisión de las bitácoras es posible afirmar que no se presentó un ataque.
- Se puede observar que el desempeño del SEI durante la jornada de marzo de 2020 tuvo problemas al inicio de ésta, pero después de 2 horas y 30 minutos, los problemas se solucionaron y el sistema terminó comportándose de manera correcta.

6. RECOMENDACIONES

Se recomienda que para posteriores versiones se cuente con el tiempo y recursos suficientes para que se realicen pruebas exhaustivas y que los simulacros se realicen con parámetros muy cercanos a los que se manejarán durante la jornada.

Se recomienda en la medida de lo posible tener los requerimientos con suficiente tiempo de anticipación y congelar el diseño a partir del 1er simulacro, a partir del cual los únicos cambios que debería haber son los relacionados con la corrección de errores.



M. en C. MARCELO PÉREZ MEDEL
Responsable del Proyecto