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 final de la Auditoría de Software previo a la jornada de votación y opinión

Periodo de evaluación:
Del 24 de febrero al 30 de marzo de 2020

Bitácora de modificaciones

Historial de versiones

Versión	Fecha	Descripción del cambio	Autor
0.0.1	25/feb/2020	Creación del documento	Marcelo Pérez Medel
0.1.0	26/feb/2020	Redacción inicial	Paulett Toledo Varela
0.2.0	27/feb/2020	Revisión del documento	Diego Rocha Zamudio
0.3.0	02/marzo/2020	Modificaciones	Axel Pantoja Romo
0.3.1	03/marzo/2020	Redacción de resultados	Paulett Toledo Varela
1.0.1	03/marzo/2020	Revisión general	Jesús Hernández Cabrera
1.1.0	04/marzo/2020	Revisión final	Marcelo Pérez Medel

Contenido

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.

De forma general, la auditoría deberá determinar si el SEI es robusto, confiable, seguro y realiza exclusivamente las operaciones y funciones para las cuales fue diseñado, de acuerdo con el análisis y diseño, garantizando la integridad en el procesamiento de toda la información.

Realizar una auditoría al SEI del IECM, que permita identificar vulnerabilidades en el sistema principal, la infraestructura que lo mantiene y los sitios web allegados al Instituto Electoral de la Ciudad de México (IECM), con lo que se podrán realizar sugerencias para el control o erradicación en el mejor de los casos de las mismas.

2. OBJETIVOS ESPECÍFICOS

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.

A. Probar todos los aplicativos desarrollados específicamente para el SEI en términos de funcionalidad.
B. Analizar las posibles vulnerabilidades de la infraestructura tecnológica del SEI.
C. Ejecutar pruebas de negación de servicios (DoS) para comprobar la robustez y disponibilidad del servicio.
D. Diseñar y ejecutar pruebas de Penetración (Pentest) al sistema e infraestructura que soporta al sistema SEI.

3. ALCANCES

A. La auditoría se realiza 24 de febrero al 30 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. METODOLOGÍA

La metodología utilizada para la realización de esta auditoría 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 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 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, tuvimos presencia en el Instituto durante todos los simulacros y monitoreamos estos desde fuera.

Los resultados se presentan a continuación:

A) Pruebas funcionales de caja negra al Sistema Electrónico por Internet.

Introducción

Esta sección contiene los resultados de las pruebas funcionales de caja negra, los cuales se obtuvieron al verificar el proceso técnico operativo mediante la aplicación de casos de prueba para los diferentes casos de uso relacionados con el sistema.

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".

El formato utilizado para registrar los casos de uso se muestra en la Ilustración 1.

	Proyecto:	Auditoría SCR 2018 IECM	
	Institución:	Universidad Nacional Autónoma de México Facultad de Estudios Superiores Aragón Centro Tecnológico Aragón	
No. Caso de prueba:	26	Nombre:	Supervisión de casillas

Diseñado por:	Jesús Hernández Cabrera.
Probado por:	
Fecha de la prueba:	
Tipo de prueba:	Software.
Precondiciones:	Haber ejecutado el caso de prueba de pantalla de inicio del módulo de supervisión del sistema.
Descripción de la prueba:	Se verificarán los flujos principales del caso de uso para visualizar la información del módulo de supervisores.

Elemento (s) a ser probado		
1		Verificación de la información del usuario mostrada en la parte superior de la pantalla.
2		Verificación del funcionamiento del menú superior "Avance en la captura de las casillas de la muestra" y de sus botones.
3		Verificación de cada una de las tablas y gráficos mostrados en las diferentes pantallas.
4		Verificación de los datos mostrados en las gráficas.

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

Hardware: Computadora en Distrito validado por el IECM con acceso a la red del sistema SCR.

Software: Navegador con acceso a la ruta del sistema.

Base de datos: Se requiere un usuario con privilegios de sólo lectura sobre las tablas de administración

Especificaciones		
Entrada	**Resultado esperado**	**Resultado obtenido**
-Uso del botón "Mapas":	-Se muestra un mapa de una demarcación territorial (inicial por defecto es Azcapotzalco) dividida por estratos, cada estrato tiene un color según su avance de casillas.	-El mapa se mostró correctamente.

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 bajo, medio y alto, 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

Las pruebas de funcionalidad se realizaron a través de 22 casos de prueba, en ellos se establece el funcionamiento técnico operativo del SEI. Cada caso de prueba contiene un número de pasos a ser revisados; para dichas pruebas se estableció un total de 165 pasos, los cuales resultan en un status:

- 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 en base de datos no se puede observar el resultado para compararlo con lo esperado.

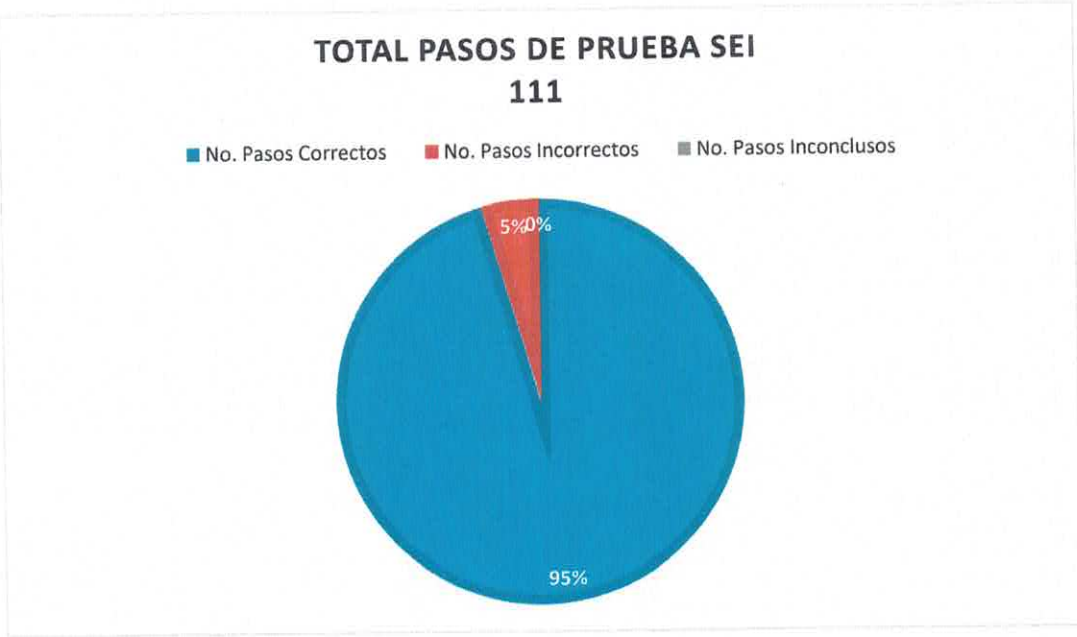
Se presenta la información obtenida al ejecutar los casos de prueba para SEI durante

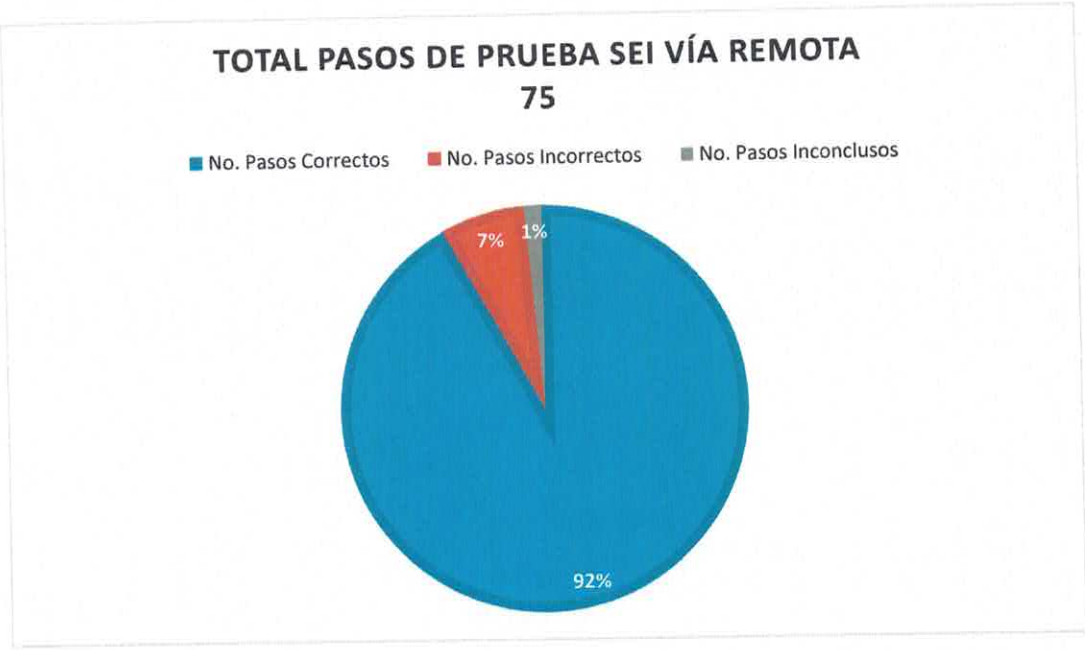
las etapas de revisión preliminar y final, posteriormente se presentan los hallazgos encontrados, los solventados y los no solventados.

Resultados de la revisión preliminar:

Al momento de la primera revisión el flujo de operación estándar funcionaba adecuadamente, pero aún faltaban detalles de la operación de flujos alternos, es decir, cuando la operación trata con excepciones.

	Pasos a probar	Correctos	Incorrectos	Inconclusos
SEI	111	106	5	0
SEI vía remota	75	69	5	1
Total	186	175	10	1





Resultados de la revisión final:

Durante la revisión final se pudo corroborar que las funcionalidades necesarias fueron implementadas y los hallazgos incorrectos o inconclusos correspondían a funcionalidades no indispensables, por lo que el no haber sido implementadas no afecta el ejercicio de la consulta. Se recomienda que en versiones posteriores sean implementadas.

	Pasos a probar	Correctos	Incorrectos	Inconclusos
SEI	106	106	0	0
SEI vía remota	69	69	0	0
Total	175	175	0	0

B) Revisión del ciclo de vida del desarrollo del sistema.

El Instituto utiliza una metodología propia y está inspirada en metodologías agiles. La metodología del Instituto incluye las etapas clásicas de análisis, diseño, construcción y pruebas.

Se recomienda que para siguientes versiones el Instituto genere una carpeta del proyecto donde integre, la descripción detallada de la metodología, así como de los documentos de modelado del sistema.

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

- Verificar que las medidas implementadas por el IECM 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 llevarán 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 IECM, puedan dar seguimiento a los mismos.

II. Validación de reporte de hallazgos. El IECM 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 IECM aplicará los diferentes controles necesarios para mitigarlos y atenderlos. Cabe señalar que el ente auditor deberá considerar dentro de su plan de trabajo, otorgar tiempo suficiente para

que el IECM pueda atender los hallazgos.

IV. Validación de la atención de los hallazgos. El ente auditor validará que el IECM 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 SEI, tuvieron como objetivo la identificación anticipada de posibles vulnerabilidades que expongan al sistema y 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 instituto.

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 que capturan y envían 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.

Entre las técnicas utilizadas se encuentran:

- Escaneos de protocolos basados en modelo TCP/IP.
- Escaneos de protocolo ICMP.
- Trazados de ruta entre IP origen e IP destino.

- Escaneos de protocolo ARP.
- Pruebas de aislamiento de segmentos de red.
- Escaneos de vulnerabilidades automatizados.

5. ***Resultado de la verificación de la aplicación de las recomendaciones***

De acuerdo al carácter de la fase de pruebas, los hallazgos no corresponden a vulnerabilidades críticas del sistema, sin embargo, todos ellos deben ser analizados y evaluados para su posterior mitigación o aceptación. Durante la ejecución de las pruebas se obtuvieron los resultados que se muestran a continuación.

Se ejecutaron pruebas de escaneo de puertos, análisis de código y análisis de vulnerabilidades, además, verificó la configuración de dispositivos de protección y balanceo para servidores, así como el aislamiento de redes y subredes pertenecientes al instituto.

Se obtuvo un hallazgo de impacto medio y tres hallazgos de impacto menor, mismos que fueron reportados al instituto para su atención y mitigación.

En relación al hallazgo de impacto medio, el día 03 de marzo del año en curso se agendó una cita en el IECM, para tratar asuntos relacionados sobre su mitigación sobre los sitios "consultaiecm.org.mx".
Debido a lo antes mencionado se realizaron pruebas sustantivas de auditoría a cada una de las capas de la infraestructura de red del IECM, teniendo como resultado que, internamente la configuración de seguridad es adecuada para su funcionamiento de manera correcta.
Se llegó a la conclusión con los resultados obtenidos de estas pruebas, que se trata de un falso positivo, debido a una configuración específica de un proveedor de servicio de red que no afecta a la operación del sistema interno. Esta configuración del proveedor es un mecanismo de seguridad para la protección de ataques DDoS el cual hace el uso de un perfil general para sus clientes y la validación de ataques

correlacionados para detectar ataques con precisión y minimizar los falsos positivos.

Revisión de configuraciones

1. Objetivos

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 y emitir recomendaciones orientadas al fortalecimiento de ésta.

2. Alcance

La auditoría se realiza del 24 de febrero al 30 de marzo de 2020.
Los alcances de este documento están establecidos en el Anexo Técnico para el sistema SEI 2020, de los cuales se consideran:

Capítulo II, inciso "f", sobre la validación de reportes y hallazgos.
Capítulo II, inciso "g", sobre la revisión de documentación y configuraciones.

3. Hallazgos

La configuración, tanto de los servidores correspondientes al sistema SEI, como de los dispositivos que los protegen se mostró aceptable en cuestiones de seguridad. La red interna del instituto tiene una segmentación aceptable y los dispositivos conectados a ella mantienen solo los puertos y servicios necesarios.

4. Conclusiones de la revisión de las configuraciones

La revisión de las configuraciones encontró servidores con parches de software actualizados, con una correcta configuración de seguridad.

D) 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 SEI y del sitio principal del IECM, durante el periodo de operación del SEI.

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 IECM, 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 IECM efectué la contramedida para la mitigación.

Tipos de ataque

Se realizaron ataques de tipo: SYN FLOOD, DNS AMPLIFICATION, ICMP FLOOD y de CAPA DE APLICACIÓN, los cuales se perpetraron a través de los protocolos TCP, UDP, ICMP y HTTP.

TIPO DE ATAQUE	PROTOCOLO
SYN FLOOD	TCP/IP
DNS AMPLIFICATION	UDP
ICMP FLOOD	ICMP
CAPA DE APLICACIÓN	HTTP

Resultados

DDoS a la página principal del instituto www.iecm.mx.

En una primera fase se realizó un ataque DDoS al sitio principal www.iecm.mx, iniciando a las 0:30 horas del día 29 de febrero con previa autorización por parte de los responsables de la infraestructura tecnológica del Instituto, y terminando esta fase a las 1:10 am del 29 de febrero de 2020.

Se generó un tráfico de al menos 400 Mbps/s y alcanzando un pico máximo de 6.4 Gbps/s (Imagen 1) y obteniendo un tiempo máximo de respuesta de 33.25 segundos.

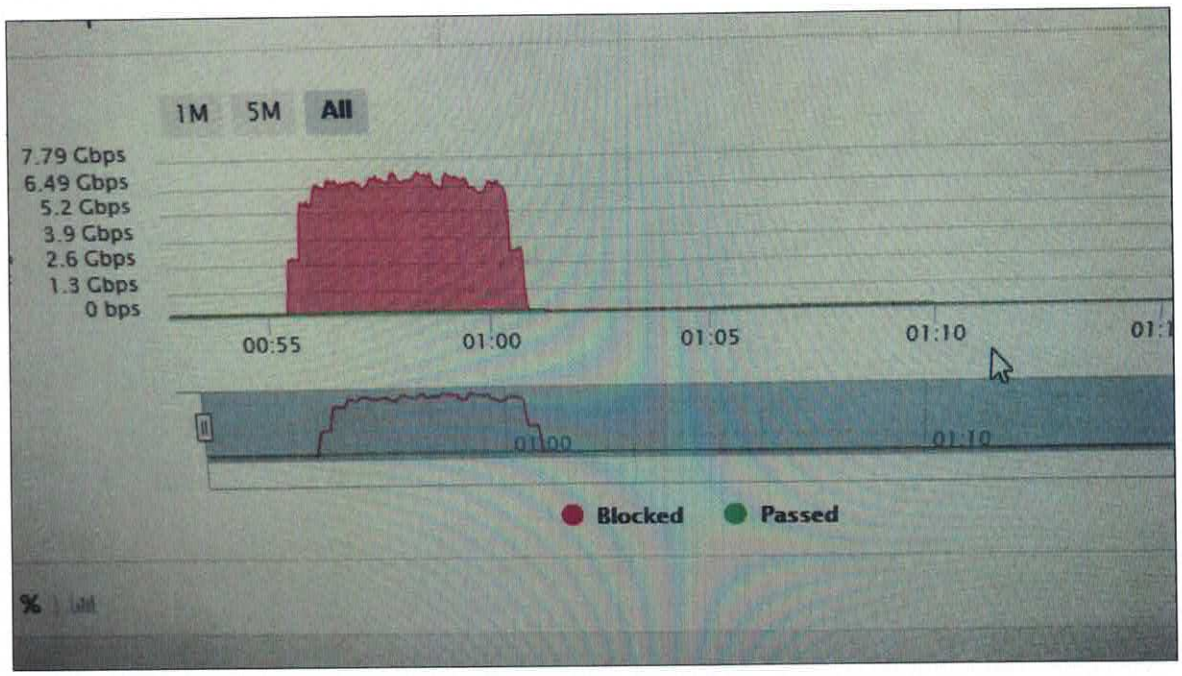


Imagen 1.- Reporte de Ancho de banda en ataque www.iecm.mx.

DDoS a la página del sistema SEI.

El ataque a los servidores web del sistema SEI inició a las 1:15 del día 29 de febrero y finalizó a las 2:05 del mismo día, generando tráfico de red y peticiones HTTP legítimas hacia el sitio. Generando un tráfico de al menos 400 Mbps/s y alcanzando un pico máximo de 21.62 Gbps/s (Imagen 2).

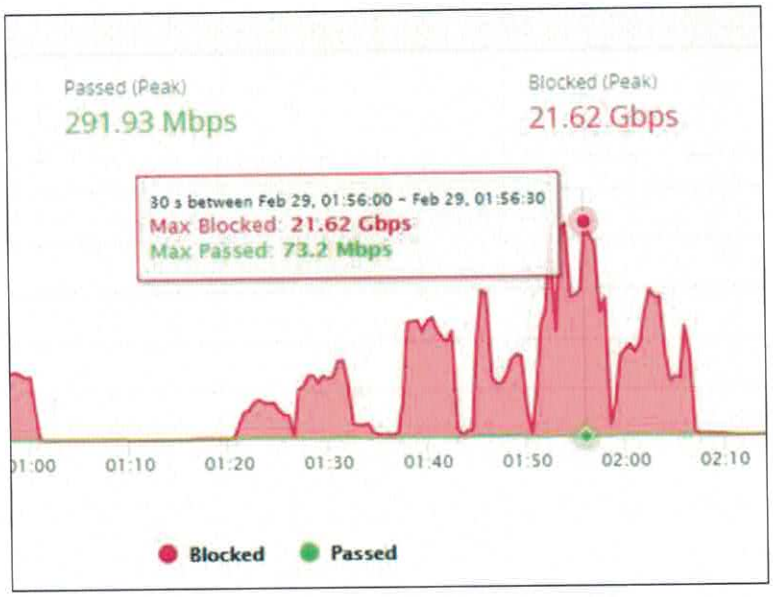


Imagen 2.- reporte de tráfico generado durante el ataque DDoS al sitio web del sistema SEI.

El tiempo máximo de carga fue de 35.18 segundos (Imagen 3) sin embargo el sistema no dejó de responder.

Aproximadamente a las 1:50, al ver que el sistema se encontraba respondiendo de forma correcta, se agregaron nuevas herramientas al ataque aumentando el tráfico hacia el objetivo, sin embargo el resultado fue el mismo, el sistema soportó la carga de forma adecuada.

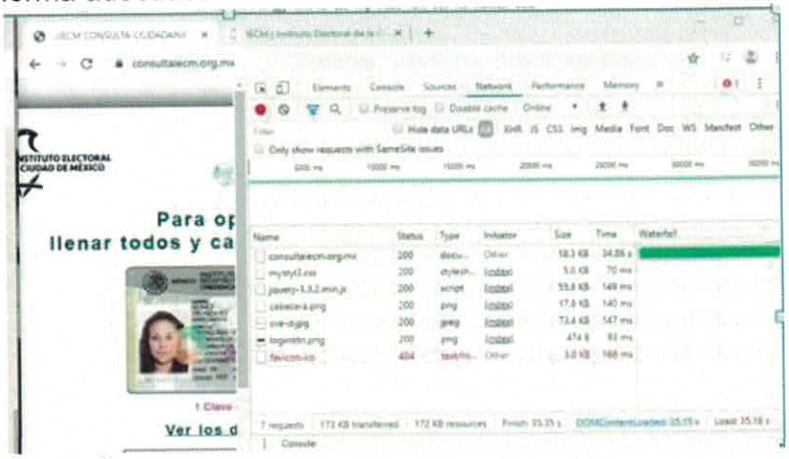


Imagen 3.- Tiempo máximo de respuesta.

A partir de todo lo anterior podemos concluir que la configuración de los sistemas de balanceo de carga funcionan de acuerdo a lo esperado y comprobaron soportar un ataque de gran escala.

Conclusiones del ataque DoS

La infraestructura web que presta servicio al sistema SEI cuenta con una configuración de balanceo de cargas y una arquitectura de protección de 3 niveles que permite el buen funcionamiento a pesar de un ataque DDoS de alto volumen. La infraestructura SEI no requiere mejoras adicionales por lo cual se recomienda mantener estas políticas de implementación para futuros sistemas.

Por otro lado, la infraestructura de la página web principal del Instituto (www.iecm.mx) requiere aprovisionar una arquitectura resiliente a mayores ataques DDoS en el futuro; el sistema SEI es totalmente independiente y no cuenta con una relación directa con la misma, por lo cual no representa en ninguno de los casos un riesgo para la operación de la jornada electoral de mes de marzo 2020.

E) Revisión del Código fuente del SEI.

Introducción

Este informe contiene los resultados de la revisión del código fuente y del archivo de aplicación (apk) de la aplicación móvil SEI.

La revisión del código de la aplicación móvil y del archivo APK fue realizada utilizando dos herramientas que analizan el código y los archivos de la aplicación de manera automática y los hallazgos verificados manualmente.

Objetivo general

Revisar el código fuente de la aplicación móvil del SEI del Instituto Electoral de la Ciudad de México, para verificar que no existan vicios ocultos en éste. De este modo se puede verificar que no existan errores que puedan provocar un funcionamiento no deseado de la aplicación ni que existan vulnerabilidades de seguridad.

Métricas de calidad

Deuda Técnica: Es el tiempo que se tendría que invertir para corregir una carencia, ya sea porque es un mal código o porque es una deuda técnica asumida previamente.

Puntuación	Descripción
A	**Deuda Técnica menor al 10%.** Se considera un proyecto estable y no requiere modificaciones.
B	**Deuda Técnica entre el 11% y el 20%.** Se considera que está en unos parámetros aceptables, pero es recomendable realizar un chequeo periódico para vigilar que no empeore.
C	**Deuda Técnica entre el 21% y el 50%.** Valores en los que el proyecto requiere algunas modificaciones. Es necesario revisar si estos errores obtenidos son falsos positivos y que estos no afecten el funcionamiento del sistema.
D	**Deuda Técnica entre el 51% y el 100%.** Es necesario que se tomen medidas correctivas para hacer más fiable el sistema. Se recomienda revisar si estos errores obtenidos son falsos positivos y que estos no afecten el funcionamiento.
E	Deuda Técnica" superior al 100%. Se requieren correcciones mayores tanto de seguridad como de buenas prácticas en la programación. Es necesario revisar si estos errores obtenidos son falsos positivos y que estos no afecten el funcionamiento del sistema.

Evidencias: Número de "malas prácticas" (violaciones) en el código. Por ejemplo, números mágicos, llamar a un método que no es un constructor con el mismo nombre que una clase etc.

Bloqueante	Errores con una alta probabilidad de impactar en el comportamiento de las aplicaciones en producción: pérdida de memoria, conexión a BD no cerrada.
Crítica	Errores con una baja probabilidad de impacto en el comportamiento del sistema o un tema que representa un fallo de seguridad: bloque catch vacío, inyección SQL, etc. El código debe ser revisado.
Mayor	Defecto de calidad que puede tener un alto impacto en la productividad de los desarrolladores: trozo de código no cubierto, bloques duplicados,

	parámetros no utilizados.
Menor	Defecto de calidad con un leve impacto en la productividad de los desarrolladores: líneas que no deberían ser tan largas, las sentencias "switch" deben tener al menos tres casos.
Info	Ni un error, ni un defecto de calidad, sólo un hallazgo.

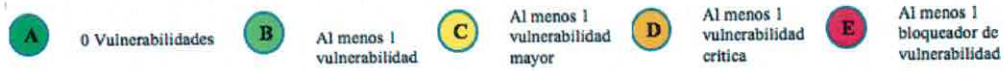
Resultados de la revisión de código

Fiabilidad: Incluye las evidencias de tipo bug y vulnerabilidades. Un bug representa algo que está mal en el código.

Numero de Bugs	Evaluación de fiabilidad	Esfuerzo de corrección
42	E	4h 55min

Seguridad: Incluye las evidencias de tipo vulnerabilidad, que representan una potencial para atacantes.

Vulnerabilidades	Evaluación de seguridad	Esfuerzo de corrección en seguridad
53	D	1d 3h



Mantenibilidad: Incluye las evidencias de tipo *code smells*, que son todas esas malas prácticas que a la larga van a provocar que cada vez sea más difícil hacer cambios en el código.

Code Smells	Evaluación de mantenibilidad	Deuda Técnica	Relación de la deuda Técnica	Esfuerzo para Alcanzar la Capacidad de Mantenimiento
1,191	A	23d	1.2 %	0

A 0 Vulnerabilidades B Al menos 1 vulnerabilidad C Al menos 1 vulnerabilidad mayor D Al menos 1 vulnerabilidad crítica E Al menos 1 bloqueador de vulnerabilidad

Duplicado: Incluye información sobre líneas de código, bloques y archivos duplicados.

19.7 %	Bloques duplicados	310
	Líneas duplicadas	9,579
	Archivos duplicados	51

Tamaño: Número total de líneas de código, sentencias, funciones clases, etc.

Líneas totales	48,563
Sentencias	10,960
Funciones	2,008
Clases	239
Archivos	272
Directorios	4
Líneas comentadas	9,086
Porcentaje de líneas comentadas	23.3 %

Complejidad: Análisis del código para calcular la complejidad ciclomática. Cuando el flujo de una función se altera, es decir, se produce un salto, este contador incrementa.

Complejidad	4,818

Evidencias: Malas prácticas (violaciones de código).

Evidencias Encontradas	1,286

Evidencias confirmadas	0
Falsos positivos	0

Observaciones:

Se encontraron varios bugs y vulnerabilidades en el código, sin embargo, se revisaron y la mayoría fueron falsos positivos ya que se encuentran en archivos generados automáticamente, algunas otras evidencias encontradas fueron resueltas o tratadas adecuadamente en el mismo código.

Sobre el resto, así como sobre los code smells, se encontraron algunos detalles sobre convenciones de programación que no se siguieron, de este modo, no afectan al funcionamiento del sistema, pero se recomienda seguir las convenciones para que el mantenimiento del software sea más sencillo.

Conclusiones de la revisión de la aplicación móvil

La aplicación móvil es adecuada para operar durante la consulta ciudadana de marzo de 2020, el sistema es seguro, hace lo que debe hacer y nada más.

F) Verificación a la infraestructura de cómputo y de comunicaciones.

Objetivo

Revisar tanto la infraestructura de cómputo como la de comunicaciones del Instituto para comprobar que son adecuados para la ejecución del SEI 2020.

Respecto a la energía eléctrica se realizaron las siguientes verificaciones:

Criterios a evaluar	Cumple	Observación
Cuentan con planta de energía	si	Una planta para el Site y otras para el Instituto en general
Tiempo de funcionamiento necesario de la planta desde su activación	si	La autonomía de la planta es de 75 horas de duración
La planta cuenta con tierra física	si	

Se cuenta con fusibles de repuesto	si	Solo uno
El Site cuenta con UPS	si	80 Kv (aproximadamente una hora de respaldo), son dos y están en redundancia
Documentos probatorios presentados		Protocolo para situación de emergencia, mantenimiento cada tres meses y compra de fusibles

También se corroboró que:

- El instituto cuenta con dos proveedores de Internet.
- Cuenta con sistemas redundantes de comunicaciones.
- Sus equipos principales cuentan con doble fuente de poder.
- El Instituto posee su Site en instalaciones propias.
- Cuentan con acceso a un site alterno.

En general se pudo comprobar que las instalaciones de cómputo y comunicaciones son adecuadas para soportar la ejecución del SEI.

6. Dictamen de la auditoría

Como resultado de las pruebas y revisiones a la infraestructura y el desarrollo del Sistema Electrónico por Internet 2020 del Instituto Electoral de la Ciudad de México, manifestamos que:

- Los servidores e infraestructura asociada a los procesos del "SEI" son razonablemente seguros.
- El **"SEI"** del Instituto Electoral de la Ciudad de México es robusto, confiable, y cumple con los requerimientos funcionales del sistema, realiza 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 y no contiene vicios ocultos.

El **"SEI"** del Instituto Electoral de la Ciudad de México está en condiciones adecuadas para operar recabar los votos y opiniones en la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021.

M. en C. MARCELO PÉREZ MEDEL
Responsable del Proyecto

M. en C. JESÚS HERNÁNDEZ CABRERA
Corresponsable del Proyecto